ARPAT
Agenzia regionale
per la protezione ambientale
della Toscana

Decreto del Direttore generale nr. 182 del 23/12/2019

Proponente: *Marco Chini*

Sira

Pubblicità/Pubblicazione: Atto soggetto a pubblicazione integrale (sito internet)

Visto per la pubblicazione - Il Direttore generale: Ing. Marcello Mossa Verre

Responsabile del procedimento: *Dott. Marco Chini*

Estensore: *Antonella Chesi*

Oggetto: Approvazione della Data protection policy di ARPAT "Modello organizzativo ARPAT" e recepimento delle linee guida per l'attuazione dei processi di Regione Toscana

ALLEGATI N.: 2

Denominazione	*Pubblicazione*	*Tipo Supporto*
Data protection policy di ARPAT "Modello organizzativo ARPAT	sì	digitale
Linee guida per l'attuazione dei processi GDPR di Regione Toscana	sì	digitale

Natura dell'atto: *immediatamente eseguibile*

Il Direttore generale

Vista la L.R. 22 giugno 2009, n. 30 e s.m.i., avente per oggetto "Nuova disciplina dell'Agenzia regionale per la protezione ambientale della Toscana (ARPAT)";
Richiamato il decreto del Presidente della Giunta Regionale n. 22 del 28.02.2017, con il quale il sottoscritto è nominato Direttore generale dell'Agenzia Regionale per la Protezione Ambientale della Toscana;
Dato atto che con decreto del Direttore generale n. 238 del 13.09.2011 è stato adottato il Regolamento di organizzazione dell'Agenzia (approvato dalla Giunta Regionale Toscana con delibera n. 796 del 19.09.2011), successivamente modificato con decreti n.1 del 04.01.2013 e n. 108 del 23.07.2013;
Visto l'"Atto di disciplina dell'organizzazione interna" approvato con decreto del Direttore generale n. 270/2011 (ai sensi dell'articolo 4, comma 3, del Regolamento organizzativo dell'Agenzia), modificato ed integrato con decreti n. 87 del 18.05.2012 e n. 2 del 04.01.2013;
Visto il Regolamento (UE) 2016/679 del Parlamento e del Consiglio Europeo del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati che abroga la Direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati – GDPR);
Richiamato in particolare l'articolo 5 del GDPR , che al paragrafo 1 enuncia i principi applicabili al trattamento dei dati personali e al paragrafo 2 pone in capo al titolare il principio di responsabilizzazione (cd accountability), in base al quale lo stesso deve assicurare, ed essere in grado di comprovare, il rispetto di tali principi;
Dato atto che la responsabilizzazione del titolare si realizza anche mediante:

- la concreta adozione, sia al momento della determinazione dei mezzi del trattamento che all'atto del trattamento stesso, di misure tecniche e organizzative adeguate ed efficaci, che tengano conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento nonché del rischio per i diritti e le libertà delle persone fisiche (privacy by design),
- l'adozione di misure tecniche ed organizzative adeguate che garantiscano che siano trattati soltanto i dati personali necessari per ogni finalità di trattamento (privacy by default),
- l'individuazione di un Responsabile della Protezione dei dati (DPO) che, tra le altre funzioni, dà indicazioni e vigila sulla corretta osservanza del GDPR all'interno dell'organizzazione del titolare;

Vista la DGRT n. 325/2018 con la quale la Regione Toscana ha provveduto alla nomina del Responsabile della Protezione dei Dati personali nella persona del dott.Giancarlo Galardi e con la quale ha messo la stessa figura a disposizione di Enti e Agenzie che ne avessero fatto formale richiesta di designazione;
Visto che la DGRT n. 325/2018 affida al DPO, tra gli altri, il compito di definire un piano di azioni per la piena applicazione del regolamento europeo e della normativa di riferimento per la Giunta regionale, avvalendosi delle competenti strutture delle Direzioni, in relazione ai trattamenti di cui sono responsabili;
Visto il decreto del Direttore generale n. 57/2018 con il quale l'Agenzia ha decretato di avvalersi della facoltà, prevista dall'art. 37, paragrafo 3 del regolamento europeo, di procedere alla nomina condivisa del RPD/DPO individuato dalla Regione Toscana;
Vista la DGRT n. 421 del 01.04.2019 con la quale la Regione Toscana ha confermato la nomina del dott.Giancarlo Galardi, fino al 31.12.2020, in qualità Data Protection Officer (DPO) e nel contempo ha messo la stessa figura a disposizione di Enti e Agenzie che ne avessero fatto formale richiesta di designazione ai sensi dell'art. 37, paragrafo 3, del regolamento (UE) 2016/679;
Visto il decreto del Direttore generale n. 77 del 14.06.2019 con il quale l'Agenzia ha proceduto alla conferma della nomina condivisa del RPD/DPO individuato dalla Regione Toscana della figura del Dr. Giancarlo Galardi;
Vista la DGRT n. 585/2018 con la quale si è previsto, tra le altre cose, di dare mandato alla Direzione Organizzazione e Sistemi informativi di redigere, con la consulenza della struttura DPO,

un primo piano di attività per un progressivo adeguamento dell'organizzazione regionale al GDPR;
Vista la DGRT 1002/2018 con la quale è stato approvato il Piano operativo di adeguamento del General Data Protection Regulation per un progressivo adeguamento dell'organizzazione regionale al GDPR;
Vista la Data protection policy regionale, basata su due macro-linee, la prima relativa all'adeguamento dell'organizzazione (messa in atto da Regione Toscana con Delibera n. 521 del 23.04.2019 della Direzione organizzazione e sistemi informativi), la seconda relativa alla messa in atto di nuovi processi GDPR, per la quale Regione Toscana ha adottato specifiche linee guida con Delibera n. 7677 del 17/05/2019 della Direzione organizzazione e sistemi informativi - Settore Ufficio Responsabile protezione dati, recepibili anche da altri Enti;
Visto il decreto del Direttore generale n. 81 del 20.06.2019 con il quale è stato approvato il Piano operativo di attività per un progressivo adeguamento dell'organizzazione e dei processi produttivi dell'Agenzia al GDPR, in cui sono riportati obiettivi, tempi e strumenti in toto o in parte derivati dal dal piano della Giunta regionale, al fine di operare congiuntamente all'interno di un quadro di comportamenti e strumenti il più omogeneo possibile condividendo un basamento di conoscenze e competenze comuni;
Visto il decreto del Direttore generale n. 82 del 20.06.2019, con il quale è stato approvato il "Registro delle attività di trattamento" al fine di un progressivo adeguemento dell'organizzazione dell'Agenzia al GDPR;
Considerato che il Piano operativo di adeguamento al GDPR di cui al sopracitato decreto n. 81/2019 prevede l'adozione della Data protection policy di ARPAT sulla base del modello organizzativo regionale di cui alla DGRT 521/2019 e delle Linee guida per l'attuazione dei processi GDPR", di cui alla DGRT 7677/2019;
Ritenuto di dover approvare la Data protection policy di ARPAT "Modello organizzativo ARPAT" (Allegato A), sulla base del corrispondente modello organizzativo regionale di cui alla DGRT 521/2019;
Ritenuto di recepire le linee guida per l'attuazione dei processi di Regione Toscana di cui alla DGRT 7677/2019 (Allegato B), da applicare con riferimento al modello organizzativo data protection di ARPAT definito in Allegato A;
Visto il decreto del Direttore generale n.192 del 30.12.2015 avente ad oggetto "Modifica del decreto del Direttore generale n. 138 del 26.09.2013 e adozione del "Disciplinare interno in materia di gestione dei rapporti tra le strutture di ARPAT ed il Collegio dei revisori";
Visto il parere positivo di regolarità contabile in esito alla corretta quantificazione ed imputazione degli effetti contabili del provvedimento sul bilancio e sul patrimonio dell'Agenzia espresso dal Responsabile del Settore Bilancio e contabilità riportato in calce;
Visto il parere positivo di conformità alle norme vigenti, espresso dal Responsabile del Settore Affari generali, riportato in calce;
Visti i pareri espressi in calce dal Direttore amministrativo e dal Direttore tecnico;
decreta

1. di approvare la Data protection policy di ARPAT "Modello organizzativo ARPAT" (Allegato A) sulla base del corrispondente modello organizzativo regionale di cui alla DGRT 521/2019;
2. di recepire le linee guida per l'attuazione dei processi di Regione Toscana di cui alla DGRT 7677/2019 (Allegato B) da applicare con riferimento al modello organizzativo data protection di ARPAT definito in Allegato A;
3. di trasmettere il presente atto alla Regione Toscana –Direzione Organizzazione e Sistemi informativi;
4. di individuare quale responsabile del procedimento il Direttore generale di ARPAT, ai sensi dell'art. 4 della L. n. 241 del 07.08.1990 e s.m.i;
5. di dichiarare il presente decreto immediatamente eseguibile, al fine di consentire il progressivo adeguamento dell'organizzazione regionale al GDPR;

Il Direttore generale
Ing. Marcello Mossa Verre*

Il Decreto è stato firmato elettronicamente da:

- Paola Querci , sostituto responsabile del settore Affari generali in data 19/12/2019
- Andrea Rossi , responsabile del settore Bilancio e Contabilità in data 20/12/2019
- Marco Chini , il proponente in data 20/12/2019
- Paola Querci , Direttore amministrativo in data 23/12/2019
- Guido Spinelli , Direttore tecnico in data 23/12/2019
- Marcello Mossa Verre , Direttore generale in data 23/12/2019

16/12/2019

ALLEGATO A

Data Protection Policy

Modello organizzativo ARPAT

Estensore: Ing. Mario Daddi

Proponente: Dott. Marco Chini

Approvazione: Ing. Marcello Mossa Verre

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

Indice generale

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

1. Scopo

Il presente documento definisce il modello organizzativo di ARPAT per la compliance con il regolamento europeo 2016/679 denominato GDPR. Nello specifico prende in esame le figure organizzative, i processi, ruoli e le responsabilità previste dal GDPR per perseguire l'obiettivo di garantire un adeguato livello di protezione nella gestione di dati personali, e descrivere come debba mutare l'assetto organizzativo dell'ente al fine di garantire nel trattamento dei dati personali la tutela dei diritti di libertà delle persone.

Si articola quindi in una breve descrizione di cosa richiede l'attuazione del GDPR, quali processi aggiuntivi debbano essere posti in essere e come questi si rapportino con i procedimenti in essere.

L'attribuzione dei compiti e delle responsabilità relative alla data protection è definita nel Disciplinare ICT e trattamenti dati di ARPAT (Decreto DG 171 del 28/12/2017), che sarà aggiornato conformemente al modello organizzativo definito nel presente atto.

2. Obiettivo del documento

Il GDPR riforma il precedente impianto normativo in materia di protezione dei dati personali – Codice Privacy, inserendo come innovativo elemento cardine il principio di Accountability (o "Responsabilizzazione") in capo al Titolare, e di eventuali Responsabili o Contitolari del trattamento, nell'adozione di misure tecniche ed organizzative adeguate ed efficaci, con l'onere di dimostrare la conformità delle attività di trattamento al GDPR stesso, garantendo la tutela ai diritti dell'interessato, nonché mettendo in atto procedure per riesaminare ed aggiornare le misure stesse.

In tale contesto assume rilievo il cambio di approccio richiesto dal Regolamento al "tema privacy" da parte del Titolare del trattamento, oggi chiamato a rimodulare i processi di gestione dei dati personali secondo **i principi di Data Protection "by design" e "by default"**, per avere la certezza che le misure tecniche e organizzative siano adottate ed integrate fin dalla progettazione (ideazione) del trattamento; per valutare i rischi di minacce che possono

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

generare violazioni dei dati personali (come riporta l'art. 1 § 2 del GDPR "il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali"); per priorizzare gli interventi, per avere la garanzia della liceità del trattamento, per monitorare costantemente le misure di sicurezza ed i trattamenti, per rendere i collaboratori, nella qualità di soggetti autorizzati, consapevoli del valore del dato attraverso la formazione e la corretta applicazione di istruzioni ad hoc ed, infine, per garantire che quest'ultimi si impegnino alla riservatezza o che abbiano un adeguato obbligo legale di riservatezza.

Pertanto, diventa opportuno un ripensamento organizzativo dell'ente cercando di ridistribuire compiti e responsabilità tra i soggetti coinvolti nel trattamento dei dati personali (vedi Titolare del trattamento, Responsabile del trattamento, persona istruita e autorizzata – ex incaricato del trattamento nel codice privacy) con la particolare attenzione di armonizzare il tutto con il nuovo ruolo DPO, introdotto dal GDPR.

Il presente elaborato vuole fornire le linee guida su come configurare un possibile futuro assetto organizzativo in materia di protezione dei dati personali.

3. Approccio di responsabilizzazione sostanziale

In riferimento alle specifiche novità introdotte dal GDPR – così come evidenziato in precedenza - si determina un approccio di responsabilizzazione sostanziale, con l'espressa indicazione di una "Data Protection compliance" basata su metodologie di valutazione del rischio e che deve essere integrata nei processi dell'Ente.

In altri termini, il Regolamento impone un "approccio preventivo, proattivo e non più reattivo", con focus su obblighi e comportamenti che prevengano in modo effettivo il possibile evento di danno, configurandosi sulle specificità dei diversi trattamenti cui si riferiscono.

4. Titolare del trattamento

Lo sviluppo delle considerazioni riportate nel paragrafo precedente ha generato la previsione specificamente contenuta nell'art. 24 del Regolamento 2016/679, rubricato "**Responsabilità del titolare del trattamento**" in cui,è previsto che, il Titolare del trattamento metta in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento sia effettuato conformemente al presente regolamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

In questo quadro, si delinea un sistema organizzativo ai fini dell'applicazione del GDPR in cui il Titolare assume il ruolo di principale attore del sistema del trattamento. Come indicato dal "Considerando n.74" del GDPR , il Titolare del trattamento assume la **responsabilità generale** per qualsiasi trattamento di dati personali che effettui direttamente o che altri abbiano effettuato per suo conto.

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

Infatti, l'art. 5 del GDPR attribuisce direttamente ai titolari del trattamento il compito di assicurare ed essere in grado di comprovare, il rispetto dei principi applicabili al trattamento dei dati personali.

Il Titolare, per rispettare il principio di accountability, deve assicurare che i dati siano sempre:

a) trattati secondo "liceità, correttezza e trasparenza";
b) raccolti per "finalità determinate, esplicite e legittime";
c) adeguati, pertinenti e limitati rispetto alle finalità;
d) esatti;
e) limitati nella conservazione;
f) trattati garantendo sicurezza e integrità.

Per l'individuazione del Titolare si deve fare riferimento – in base a quanto previsto dall'art. 4 del GDPR – "alla persona fisica, persona giuridica, autorità pubblica, servizio o altro organismo" che determina le finalità e i mezzi del trattamento di dati personali, autonomamente o in regime di contitolarità.

Con riferimento ad un Ente, va specificato che la necessaria identificazione della " persona fisica, persona giuridica, autorità pubblica, servizio o di altro organismo" quale titolare o contitolare del trattamento non preclude l'applicazione dei principi generali in materia di formazione della volontà dell'ente e di delega di funzioni, nel senso che la volontà del "titolare/contitolari" sarà formata, anche agli effetti della disciplina della protezione dei dati, tenendo conto delle ordinarie attribuzioni degli organi previsti dall'atto costitutivo e dallo statuto.

In tal senso, sono da considerare tutte le caratteristiche specifiche che influiscono sul processo di determinazione delle finalità e dei mezzi del trattamento di dati personali.

In conclusione, le specifiche del modello organizzativo amministrativo che si delinea costituiscono l'elemento qualificante per determinare le scelte della volontà (e le modalità di esercizio delle stesse) attraverso la struttura amministrativa che le compete, incluse quelle relative alle finalità e ai mezzi del trattamento di dati personali.

5. Data Protection Officer (DPO) e Ufficio DPO

Il Data Protection Officer – DPO –, altrimenti noto come Responsabile della protezione dei dati, è una nuova figura di riferimento, per tutto ciò che attiene la materia di protezione dei dati personali, e si affianca al Titolare o al Responsabile del trattamento e nei rapporti esterni con le Autorità di controllo e con gli Interessati.

Il DPO è una figura la cui nomina è obbligatoria, tra l'altro, per gli enti pubblici.

Il DPO è parte dell'organizzazione Data Protection dell'Ente, di cui non necessariamente deve essere un dipendente, ben potendo tale ruolo essere assolto da un soggetto esterno identificato dal Titolare o dal Responsabile del trattamento.

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

Il Gruppo di lavoro , costituito da tutti i rappresentanti dei Garanti europei, ha più volte ribadito l'importanza della figura del DPO quale pilastro della responsabilizzazione che agisce quale coordinatore della conformità al GDPR.

Il DPO è incaricato, dal Titolare del trattamento, di svolgere almeno i seguenti compiti e funzioni:

a) informare e fornire consulenza al Titolare del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal regolamento (UE) 2016/679, nonché da altre disposizioni nazionali o dell'Unione relative alla protezione dei dati;

b) sorvegliare l'osservanza del regolamento (UE) 2016/679, di altre disposizioni nazionali o dell'Unione relative alla protezione dei dati nonché delle politiche del Titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del regolamento (UE) 2016/679;

d) cooperare con il Garante per la protezione dei dati personali;

e) fungere da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del regolamento europeo, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

f) fungere da punto di contatto per gli interessati, per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.

Il DPO riferisce direttamente al Titolare del trattamento.

Il DPO, se nominato come soggetto esterno all'Agenzia, è supportato internamente da un ufficio , denominato **Ufficio DPO.**

Non possono essere nominati DPO soggetti che ricoprono ruoli nell'organizzazione che possono determinare potenziali conflitti d'interesse o il mancato rispetto dei principi di controllo, con particolare attenzione al principio della **separazione** delle funzioni.

Il DPO non può rivestire ruoli che comportino la definizione di finalità e mezzi di trattamento, né può ricevere istruzioni dal Titolare sulle modalità di esecuzione dei propri compiti.

Il Titolare del trattamento e il Responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

Il sistema dei flussi informativi è strutturato in base ai seguenti punti principali:

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

a) ogni direttore, dirigente, posizione organizzativa e/o altre eventuali figure di coordinamento sono tenuti a comunicare al DPO ogni evento rilevante ai fini dell'applicazione del GDPR

b) i responsabili della Struttura organizzativa interna per la sicurezza dei trattamenti con mezzi elettronici e della Struttura organizzativa per la sicurezza dei trattamenti cartacei (qualora nominati) devono comunicare tempestivamente al DPO le evidenze di ogni attività di controllo e/o di altra natura rilevante ai fini dell'applicazione del GDPR

c) i dati di contatto del DPO da pubblicare dovranno ricomprendere le informazioni che possono consentire agli interessati e al Garante di raggiungerlo con facilità: recapito postale, numero telefonico dedicato e/o indirizzo mail dedicato

d) il primo riferimento operativo per le richieste degli interessati è l'URP, cui sono delegate le attività di comunicazione di front end. Il DPO provvederà a fornire le indicazioni necessarie per la formazione degli addetti dell'URP per curare le necessarie attività d backoffice.

e) le richieste più specifiche che richiedono un parere da parte dell'Ufficio DPO, avvengono per via telematica secondo le indicazioni riportate sul sito istituzionale di ARPAT.

In relazione al ruolo previsto dal legislatore europeo che configura il DPO come un consulente indipendente, il compito del DPO nell'ambito delle attività di verifica è quello di vigilare affinché il sistema dei controlli preventivi (l'insieme delle misure di sicurezza tecniche e organizzative e ogni altro presidio di controllo applicato dall'Ente) nel suo complesso sia adeguato a mitigare i rischi riferibili al diritto alla protezione dei dati personali e a mantenere nel tempo la propria efficacia nel mantenere a livello accettabile i rischi di volta in volta rilevati e/o emergenti. Per tale attività si avvale del Security Manager.

In sostanza, non competono al DPO i controlli operativi sull'osservanza del regolamento. Per controlli operativi si intendono quei controlli sull'operato dei dipendenti assegnati alla struttura di cui il dirigente è responsabile.

I controlli operativi spettano ai dirigenti, o a loro delegati a norma del contratto di lavoro, in riferimento ai trattamenti di dati personali svolti nel settore di cui sono responsabili. Per tali attività di controllo in merito alla correttezza delle operazioni e non dei comportamenti, possono avvalersi del supporto dei Data Protection Specialist di ARPAT.

Le evidenze di tutti i controlli e di ogni altra attività di verifica effettuata, rilevante ai fini del GDPR, devono essere comunicate al DPO.

In riferimento alle evidenze dei controlli svolti, alle eventuali segnalazioni ricevute, alla verifica di documentazione e/o ad ogni altra informazione acquisita rilevante ai fini del GDPR, il DPO può:

a) riservarsi di chiedere approfondimenti ai soggetti competenti per i controlli;

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

b) intervenire con una pluralità di azioni idonee a favorire l'osservanza delle prescrizioni del GDPR (a titolo esemplificativo, si vedano le ipotesi di intervento in ordine al controllo del registro dei trattamenti, così come indicate nelle Indicazioni Operative per il Registro delle attività di trattamento);

c) disporre ulteriori controlli ai fini del processo di accountability – da effettuarsi dall'Ufficio DPO o da altri soggetti specificatamente designati dal DPO stesso - negli ambiti di competenza assegnati dal legislatore europeo (sorvegliare l'osservanza del regolamento, nonché delle altre disposizioni europee o di diritto interno in materia di protezione dati; sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e attività di controllo).

Nel rispetto di quanto disposto dall'art. 39, secondo paragrafo, del GDPR ("Nell'eseguire i propri compiti, il DPO considera debitamente i rischi inerenti al trattamento…") il DPO può definire un ordine di priorità nelle attività da svolgere in relazione a quelle che hanno come ambiti di riferimento quelli che presentino maggiori rischi in termini di protezione di dati (c.d. Piano attività Risk Based).

Allo scopo di svolgere le proprie funzioni, il DPO può:

a) partecipare agli incontri organizzati dalla Direzione generale, valutando quali tra essi rivestano rilevanza per il corretto svolgimento dei propri compiti. A tal fine, in osservanza al principio di Data Protection by Design, ogni qualvolta siano in trattazione argomenti e attività che comportano trattamento di dati personali, occorre, secondo le regole organizzative dell'ente, darne comunicazione al DPO, che valuterà se e come intervenire;

b) accedere a tutta la documentazione e a tutte le sedi rilevanti dell'Ente per lo svolgimento dei propri compiti;

c) Il DPO – ai sensi dell'art. 38 del GDPR - deve essere dotato delle risorse necessarie per lo svolgimento efficace dei propri compiti, così come indicati all'art. 39 del GDPR, per accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.

Il DPO svolgerà in autonomia le proprie attività, con il potere di intervenire per il rispetto della normativa.

6. Responsabile del trattamento

Il Regolamento definisce il Responsabile del trattamento come la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare (art. 4, § 8; art. 28).

L'approccio basato sul rischio e misure di accountability del GDPR influenza anche la figura del Responsabile del trattamento, al quale sono assegnati nuovi compiti e che condivide in certa

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

misura le responsabilità del Titolare, in riferimento al risarcimento del danno a terzi, ed è oggetto di autonome sanzioni amministrative.

Il Responsabile risponde per danno se non ha adempiuto agli obblighi previsti dal regolamento, ma anche se ha agito senza rispettare le istruzioni del Titolare.

Il Responsabile è soggetto anche a obblighi risarcitori per mancanze ad esso ascrivibili e, in caso disattenda le istruzioni del Titolare al punto da individuare - con i dati che ha ricevuto in affidamento - proprie finalità del trattamento, diventa a sua volta Titolare autonomo, con conseguente applicazione del quadro di riferimento - anche sanzionatorio - ben più “pesante”, rispetto a quello relativo ad una semplice violazione degli obblighi contrattuali assunti con il Titolare.

Il Responsabile del trattamento deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate – in primis agli standard stabiliti dal Titolare - in modo tale che il trattamento soddisfi i requisiti previsti dal GDPR e garantisca la tutela dei diritti dell’interessato.

I trattamenti svolti da un Responsabile devono essere disciplinati da un contratto o altro atto giuridico stipulato con il Titolare. Il contratto deve regolare gli elementi essenziali del trattamento di dati personali curato dal Responsabile, con particolare riferimento a:

a) materia disciplinata;
b) durata del trattamento/i;
c) natura e finalità del trattamento/i;
d) tipo di dati personali;
e) categorie degli interessati coinvolti;
f) nonché a tutti gli altri elementi indicizzati all’art. 28, comma 3, GDPR; definendo in modo chiaro quali siano gli obblighi e i diritti del Titolare e quali quelli del responsabile, tenendo nel debito conto l’attività di controllo propria del Titolare.

7. Autorizzati

Ai fini di individuare gli "autorizzati", al trattamento dei dati personali, si deve far riferimento alle seguenti disposizioni del GDPR:

1. trattasi è di persone soggette alla “autorità diretta del Titolare o del Responsabile” (art. 4, § 10)
2. gli stessi non possono trattare dati personali del Titolare per il quale operano se non dietro istruzione fornita dal Titolare o dal Responsabile del trattamento, salvo che lo richieda il diritto dell’Unione o degli Stati membri (artt. 29 e 32 § 4).

Quindi per trattare i dati bisogna essere soggetti istruiti e autorizzati.

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

8. La compliance al GDPR

Passiamo a definire come le figure previste dal GDPR si mappano con ruoli e responsabilità dell'organizzazione di ARPAT, per rispondere al dettato regolamentare europeo. Segue un breve riepilogo delle figure previste dal GDPR.

8.1 Le figure e le responsabilità nell'organizzazione

Il Regolamento europeo 2016/679 (GDPR) richiede che le organizzazioni adottino una struttura (ruoli e funzioni) e procedimenti che garantiscano intrinsecamente, così come previsto all'art. 1 (C1-14, C170, C172), la protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché la libera circolazione di tali dati, proteggendo i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.

Questo in quanto le finalità sono la protezione per l'affermazione di diritti delle persone fisiche, commisurata alla riduzione dei rischi derivanti dall'uso improprio o illecito di dati personali.

A tale scopo il GDPR introduce figure organizzative, con ruoli e responsabilità precisi, e fissa alcuni principi organizzativi atti a vincolare i comportamenti in modo che siano coerenti con le finalità del regolamento stesso.

8.2 Figure previste esplicitamente o implicitamente dal regolamento

Titolare del Trattamento dati, art. 24 GDPR (C74-C78) (in inglese Controller) è colui che ha la responsabilità, fra le altre, di mettere in atto misure tecniche ed organizzative *adeguate* per garantire, ed essere *in grado di dimostrare* (principio della accountability), che il trattamento è effettuato in modo conforme al regolamento. A lui è demandata in via diretta o indiretta la tutela dei diritti e delle libertà fondamentali della persona fisica a cui si riferiscono i dati personali che vengono trattati. Decide in ordine a finalità e mezzi (questi ultimi parzialmente delegabili a responsabili) dei trattamenti di propria competenza e ha la responsabilità di tenuta del registro dei trattamenti ex art. 30 GDPR (C82).

Delegato del Titolare, Art .2-quaterdecies, comma 1, d.lgs. 196/2003 è la persona fisica, con atto espresso dal Titolare, a svolgere le sue funzioni a norma del GDPR.

Responsabile del Trattamento, Art. 28 GDPR (C81) (in inglese Processor) Persona fisica o giuridica, diversa dal Titolare ed esterna all'organizzazione dello stesso, che eventualmente effettua trattamenti per conto del Titolare. Il rapporto fra Titolare e Responsabile, ove previsto, deve essere regolato da apposito contratto o altro atto bilaterale. Al Titolare spetta l'onere e la responsabilità di indicare al responsabile le modalità di trattamento e le relative istruzioni, nonché di controllare che siano rispettate.

Gli autorizzati, art .2-quaterdecies, comma 2, d.lgs. 196/2003 sono le persone autorizzate dal Titolare al trattamento dei dati: al Titolare compete di dare, oltre che l'autorizzazione, anche le istruzioni e un'adeguata formazione in merito alle misure da adottare nella esecuzione del trattamento.

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

Data Protection Specialist, figura implicitamente prevista dal GDPR, quando prevede e mette in capo al Titolare, responsabilità e attività che prefigurano competenze tecniche specialistiche, non riconducibili direttamente alle competenze richieste per svolgere il ruolo di Titolare. In particolare la valutazione dei rischi (DPIA Art. 35 C84, C89-C93, C95), l'individuazione dei trattamenti partendo dai processi dell'organizzazione e andandone ad individuare i riferimenti che ne determinano la liceità, la determinazione della misura dei rischi di natura tecnica ed organizzativa, ecc. Una figura che abbia competenze organizzative, giuridiche e tecnologiche, o coadiuvata da altre, quale punto di riferimento multidisciplinare a supporto del Titolare, del DPO, dei Responsabili di struttura e degli incaricati.

Security manager/Data Security Officer**,** figura implicitamente prevista dal GDPR, per garantire quanto previsto alla sezione 2 "sicurezza dei dati personali" , per supportare il Titolare nei suoi compiti di supervisione e controllo delle misure di sicurezza adottate, per determinarne la loro adeguatezza nel tempo e per garantire il rispetto del principio di separazione delle responsabilità fra chi le misure le deve attuare, il *Responsabile per la transizione al digitale* dell'organizzazione o il *Responsabile del trattamento*, e chi invece deve controllarle.

Il DPO (Data Protection Officer), o Responsabile della protezione dei dati, previsto sezione 4 del GDPR art. 37-39. Svolge azione di promozione, consulenza e verifica per il corretto comportamento organizzativo in ottemperanza al regolamento. Mantiene relazioni con l'autorità garante e funge da punto di contatto con gli interessati per agevolare l'esercizio dei loro diritti.

L'Ufficio DPO, struttura non esplicitamente prevista nel GDPR ma derivante dall'esigenza: di essere un punto di competenza multidisciplinare a supporto del Titolare e suoi delegati, di essere punto di contatto con gli interessati, di essere punto di riferimento organizzativo di supporto alle interlocuzioni con il Garante.

8.3 Come si mappa l'organizzazione GDPR con l'organizzazione di ARPAT

Il Direttore Generale assume, a norma dell'Art. 4 punto 7 del GDPR, il ruolo di *Titolare dei trattamenti* afferenti alle finalità dell'ente ARPAT.

Il Direttore tecnico e il Direttore amministrativo assumono, con il presente atto, la figura di *Delegato del Titolare* per i trattamenti di loro diretta responsabilità. A tal fine curano le seguenti attività:

1. la regolamentazione e il controllo dei trattamenti;

2. la predisposizione e aggiornamento di:

- informative per gli interessati;
- Registro Trattamenti;
- Valutazione d'impatto sulla protezione dei dati (DPIA).

Le informative, il Registro Trattamenti e la DPIA sono approvati dal Titolare.

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

I Responsabili di struttura assumono, con il presente atto, la figura di *Delegato del Titolare* per i trattamenti di loro diretta responsabilità.

Il DPO (Data Protection Officer) è stato nominato con Decreto DG n. 57/2018. L'incarico è stato confermato alla scadenza con Decreto DG n. 77 del 14/06/2019.

L'Ufficio DPO è individuato, con il presente atto, all'interno del settore SIRA. Nell'ufficio sono collocati i *Data Protection Specialist*, dipendenti opportunamente formati in materia di data protection.

Il Security Manager /Data Security Officer è stato nominato con Decreto DG 137 del 27/12/2018.

I Dipendenti assumono, con il presente atto, il ruolo di *Autorizzati al trattamento* ai sensi dell'art .2-quaterdecies, comma 1, D. Lgs. 196/2003.

9. I Processi GDPR

La compliance al GDPR si sostanzia nella messa in atto di un modello organizzativo che si innervi nella realtà organizzativa dell'ente e di processi specifici finalizzati alla costante verifica dei dati trattati e della adeguatezza delle misure adottate e commisurate alla valutazione dei rischi. Altro aspetto che la compliance deve garantire è l'esercizio dei diritti degli interessati.

9.1 Processo: Data protection by design e by default

Questo processo riguarda il rispetto di quanto disposto art. 25 del GDPR, ed è rappresentato da tutte quelle analisi e valutazioni da effettuare al momento della emissione di un qualsivoglia atto che comporti come conseguenza un trattamento di dati personali. Nel caso in cui l'atto prefiguri il trattamento di dati personali devono essere valutati, al livello di dettaglio commisurato alla tipologia di atto, i seguenti aspetti:

a) Individuazione del trattamento sotteso e del processo organizzativo che si va a ipotizzare o realizzare, modificare, integrare;

b) I soggetti organizzativi coinvolti e le differenti figure dell'organizzazione GDPR;

c) Le relative misure di sicurezza.

Tale processo deve essere vincolante nella produzione di un qualsivoglia atto.

Pertanto si procede alla modifica della procedura dell'iter di approvazione degli atti al fine di inserire, a cura del dirigente promotore, una fase di verifica degli impatti GDPR dell'atto, così che se l'atto prefigura il trattamento dei dati personali, l'atto deve essere obbligatoriamente corredato di informazioni aggiuntive ai sensi della disciplina in materia di protezione dei dati personali.

Tale processo è descritto nel documento "Linee guida per la Data Protection by design e by default".

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

9.2 Processo: Mantenimento del registro dei trattamenti

L'art. 30 del GDPR (C82) pone in capo al Titolare la responsabilità di tenere un registro delle attività di trattamento. N ell'organizzazione di Arpat sono individuati il Direttore tecnico e il Direttore Amministrativo, ciascuno per i trattamenti di propria competenza.

Pertanto occorrerà definire un modello organizzativo che garantisca:

1. La gestione del ciclo di vita del trattamento.
2. Il collegamento con l'organizzazione dell'ente al fine di mantenere allineate le strutture, le competenze e le persone a seguito di variazioni organizzative, quali cambio di dirigenti, cambio di competenze delle strutture, cambio di personale autorizzato, ecc.
3. Il collegamento con i processi produttivi dell'ente in quanto i trattamenti sono segmenti di tali processi finalizzati al trattamento di dati personali. Il riferimento al processo risulta importante in quanto è sulla base del processo, e non del singolo trattamento, che risulta opportuno fare la valutazione dei rischi e la esecuzione di vere e proprie DPIA. Analizzando i singoli trattamenti, può accadere di sottovalutare o sopravvalutare rischi, o di dover eseguire più DPIA, una per ogni trattamento, con dispendio di costi e tempi, quando sarebbe stato possibile farla una sola volta sull'intero processo (in senso conforme, art 35 comma 1): "… Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi").
4. Il collegamento con gli asset, intesi come applicazioni IT, basi di dati e strutture tecnologiche di supporto, ma anche archivi cartacei e relativi supporti, al fine di determinare le misure di sicurezza.
5. Il collegamento con le procedure di assegnazione dei diritti di accesso a dati e funzioni al fine di riportare sui trattamenti correlati, i nominativi degli autorizzati e i relativi privilegi nel trattamento.

Questo prefigura un aggiornamento della procedura IT di gestione dei trattamenti in una logica di processo garante della rappresentazione fedele della realtà.

La gestione dei trattamenti e la loro registrazione nei fatti si configura come un sotto-processo del processo di Data Protection by Design.

Per la descrizione di dettaglio si rimanda alle "linee guida per il mantenimento del registro dei trattamenti" (Appendice G delle "linee guida per la data protection by design e by default").

9.3 Processo: Formulazione e gestione della DPIA

Il GDPR all'art.35, in coerenza con il principio di sostanziale responsabilizzazione, basato sull'analisi dei rischi, prevede lo strumento della DPIA quale processo mirato alla valutazione degli impatti conseguenti ai rischi rilevati e alla determinazione delle misure finalizzate alla loro riduzione.

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

La DPIA viene individuata come processo obbligatorio in tutti quei casi in cui, in particolare con l'uso delle di nuove tecnologie, si può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Il Garante Nazionale con provvedimento n. 467 del 11 Ottobre 2018 (Pubblicato sulla Gazzetta Ufficiale n. 269 del 19 novembre 2018) ha individuato, così come previsto all'art. 35 comma 4 del GDPR, le tipologie di trattamenti per i quali la DPIA è un adempimento obbligatorio:

1. Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso App, relativi ad “aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato.
2. Trattamenti automatizzati finalizzati ad assumere decisioni che producono “effetti giuridici” oppure che incidono “in modo analogo significativamente” sull’interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l’utilizzo di dati registrati in una centrale rischi).
3. Trattamenti che prevedono un utilizzo sistematico di dati per l’osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell’informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d’uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.
4. Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull’esercizio di un diritto fondamentale (quali i dati sull’ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell’interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).
5. Trattamenti effettuati nell’ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell’attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn.3,7 e8).
6. Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

7. Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogni qualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01 .
8. Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.
9. Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment).
10. Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.
11. Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.
12. Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

La decisione o meno di effettuare una DPIA e il suo svolgimento è in capo al Titolare o suo delegato che si consulta con il DPO.

I contenuti minimi di una valutazione di impatto sono descritti all'art. 35 comma 7 del GDPR a cui si rimanda.

Il Titolare nello svolgimento della DPIA, se del caso, così come previsto all'art. 35 comma 9 richiede il parere degli interessati o dei loro rappresentanti.

In sintesi il processo di DPIA è competenza del Titolare o suo delegato, che si avvale della consultazione con il DPO ed è mirato ad evidenziare e documentare in modo chiaro i rischi, le misure di sicurezza adottate per mitigarli e i rischi residui. La DPIA è mantenuta aggiornata dal Titolare allorquando si modifichi il processo, intervengano incidenti che mettano in luce possibili debolezze del sistema non considerate, si evidenzino minacce non prese in considerazione, ecc..

La formulazione della DPIA si configura come un sotto-processo del processo di Data Protection by Design da mettere in atto qualora la tematica in questione la richieda.

9.4 Processo: Gestione degli incidenti

È opportuno che siano definite delle figure per il presidio del processo di raccolta, gestione e analisi degli incidenti fra cui anche il processo di Data Breach previsto dal GDPR.

Il Security Manager, assistito dai data protection specialist, provvede a:

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

1. mantenere un registro degli incidenti;
2. valutare l'impatto sulla continuità del servizio coordinandosi con l'eventuale responsabile della continuità operativa;
3. supervisionare il gruppo di intervento e gli specialisti nelle attività di contrasto degli incidenti durante le fasi di emergenza;
4. segnalare al DPO possibili vulnerabilità e/o incidenti in ambito di trattamento di informazioni personali;
5. analizzare lo storico degli incidenti insieme agli specialisti al fine di identificare delle soluzioni stabili in grado di contrastare le vulnerabilità emerse;
6. comunicare al Responsabile della sicurezza (quando presente) o ai responsabili dello sviluppo dei sistemi informativi o delle infrastrutture, la sintesi delle vulnerabilità emerse dal registro degli incidenti e le soluzioni intraprese per il loro contrasto;
7. supportare il Titolare del trattamento (o a suo delegato) e il DPO nel processo di notifica del Data Breach al Garante e alle altre autorità competenti;
8. supportare il Titolare del trattamento (o suo delegato) e il DPO nel valutare la necessità di procedere anche alla comunicazione dell'incidente a tutti gli Interessati.

9.5 Processo: Accountability

In riferimento all'approccio di responsabilizzazione sostanziale introdotto dal GDPR si determinano rilevanti ulteriori novità anche in merito al sistema organizzativo nel suo complesso.

Il Regolamento, come già indicato in precedenza, prevede espressamente una compliance basata su metodologie di valutazione del rischio e che deve essere integrata nei processi dell'Ente.

In altri termini, rispetto al Codice Privacy, si passa dalla richiesta di una somma di adempimenti obbligatori ad un approccio per processi e ad una protezione dei dati personali in ottica Risk Based.

L'approccio per processi favorisce la visione globale dell'organizzazione, rappresentandola attraverso un insieme di processi tra loro interconnessi.

Per un'efficace applicazione del GDPR e del rispetto del principio di accountability, in particolare, è opportuno che il sistema organizzativo includa la rilevazione dei processi, che evidenzi il complesso delle attività svolte, la loro sequenza e le modalità con cui sono corrispondentemente effettuate.

Adempimenti rilevanti ai fini GDPR quali il censimento dei trattamenti dei dati personali, la correlata predisposizione del registro dei trattamenti e il mantenimento dello stesso aggiornato e allineato ad ogni eventuale nuovo trattamento avviato e/o variazione intervenuta nei

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

trattamenti preesistenti implicano che tutte le attività svolte dall'Ente siano analizzate e siano continuamente monitorate.

L'efficacia di tali analisi può essere maggiore se condotta con il supporto preventivo della mappatura dei processi, in modo da poter più facilmente identificare gli ambiti di attività effettivamente svolte e ogni eventuale trattamento correlato che, in ragione della natura e delle peculiarità dell'attività stessa, risultano potenzialmente esposti a rischi rispetto al diritto alla protezione dei dati personali.

Peraltro, già altre norme – tra cui la Legge 190/2012 ("Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione") – richiedono un modello organizzativo che includa un approccio per processi, ai fini di meglio identificare e prevenire i rischi verso cui sono potenzialmente esposte le attività dell'Ente.

In particolare, riveste particolare importanza l'identificazione e mappatura dei processi in modo unitario, a prescindere dall'istanza contingente che ne motiva la realizzazione (quali l'applicazione di una specifica norma o la risposta ad una puntuale esigenza gestionale).

Infatti, i processi – rappresentando come effettivamente sono svolte le attività dell'Ente – se declinati con un approccio unitario (valido per tutto l'Ente e per tutte le casistiche applicative) e con la stessa metodologia di rilevazione consentono una più semplice individuazione delle responsabilità, dei potenziali rischi cui sono esposti gli obiettivi di ogni processo e del livello di adeguatezza delle misure di sicurezza, di prevenzione e/o di controllo esistenti.

Inoltre, lo stesso "linguaggio" consente per ogni processo - da un lato - la confrontabilità del grado di rilevanza dei diversi rischi, indipendentemente dall'ambito operativo in cui possono manifestarsi e dall'altro, la rilevazione di ogni misura tecnica e organizzativa applicata ai fini della mitigazione dei rischi rilevati, con la conseguente possibilità di razionalizzare le misure di prevenzione.

In conclusione, l'approccio unitario per processi riveste un ruolo cruciale per l'implementazione e l'aggiornamento di un Sistema Organizzativo in grado di realizzare una gestione dei rischi efficace ed efficiente.

Il Modello organizzativo richiesto dal GDPR rientra nella categoria dei ***Compliance Program***, cioè di modelli organizzativi atti alla prevenzione di rischi di compliance cui è esposto l'Ente.

Per rischio di compliance si intende il rischio di incorrere in sanzioni, subire perdite o danni reputazionali in conseguenza della mancata osservanza di leggi, regolamenti o provvedimenti.

Il Modello per l'applicazione del GDPR, come gli altri Compliance Program, prevede per la propria realizzazione 2 macrofasi:

a) Risk Assessment (identificazione e valutazione dei rischi);

b) Verifica ed eventuale implementazione del Sistema dei controlli (idonei a prevenire i rischi individuati nella macrofase 1).

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

Il Sistema dei controlli, con riferimento al GDPR, può essere correlato alle misure tecniche e organizzative adeguate a garantire che il trattamento è effettuato in conformità al Regolamento stesso.

Il Sistema dei controlli, o Sistema di controllo interno, in base ai framework di riferimento più diffusi è composto da diversi elementi di controllo generale. Inoltre, le componenti del Sistema di controllo interno devono integrarsi tra loro nel rispetto di una serie di principi di controllo.

Il *Sistema organizzativo costituisce uno degli elementi di rilievo del Sistema di controllo interno*: tener in considerazione le correlazioni del Sistema organizzativo con gli altri componenti del Sistema di controllo interno può consentire di:

1. rafforzare la capacità di mitigazione dei rischi delle misure organizzative;
2. ampliare lo spettro di compensazione/adattamento delle misure organizzative rispetto ad eventuali criticità – temporanee o durature – delle misure tecniche per la prevenzione dei rischi;
3. favorire un approccio coordinato all'applicazione dei diversi Compliance Program e, conseguentemente, la loro efficacia di prevenzione dei rischi individuati.

Il principio di accountability sancito dal regolamento europeo in materia di protezione dei dati richiede che l'organizzazione e i processi, siano impostati in modo tale da rendere possibile la attività di "rendere conto" delle misure messe in atto per la protezione dei dati.

Principio che si lega fortemente con l'altro della data protection by design in quanto se nella progettazione di nuove iniziative si tiene presente la tematica della protezione dei dati fin dall'inizio e aggiornata nel tempo, l'attività di rendicontazione delle scelte diviene una logica conseguenza della lettura delle decisioni prese e delle relative motivazioni. Se così non fosse e si dovesse rendere conto di quanto fatto solo a valle della rilevazione degli incidenti, ovviamente richiederebbe una ricerca a ritroso non certo agevole sia nel risultato sia nei tempi mettendo il Titolare e tutta l'organizzazione in situazioni sanzionabili a norma del GDPR.

L'organizzazione dell'ente può essere chiamata a rendere conto in varie circostanze:

a) su istanza del Garante in attività ispettiva o a seguito di segnalazioni o denunce;
b) su istanza degli interessati nell'esercizio dei loro diritti;
c) su istanza del DPO in attività di monitoraggio o a seguito di segnalazioni da parte degli interessati.

In particolare l'attività di "rendere conto" si sostanzia:

1. individuazione del processo in esame;
2. rispetto dei principi generali applicabili ai trattamenti;
3. misure di sicurezza messe in atto sulla base del processo di assessment e di valutazione degli effetti (danni) sulle libertà e i diritti individuali delle persone fisiche, dei rischi, delle minacce e della probabilità di accadimento.

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

All'interno del Processo di Data Protection by design and by default, è prevista la costituzione di un **dossier data protection** per ogni processo che tiene traccia delle scelte, delle misure e delle motivazioni che hanno portato alla loro determinazione. Il dossier è tenuto aggiornato come risorsa condivisa dalle diverse figure responsabili dei vari ambiti.

Questo sia che sia stata effettuata a norma dell'art. 35 (C84,C89-C93, C95) una specifica DPIA, sia che non sia stata effettuata in quanto ritenuta non necessaria.

9.6 Processo: Garanzia e tutela dei diritti degli interessati

Il GDPR dedica l'intero Capo III ai diritti dell'interessato ed in particolare:

1. art. 12: trasparenza e modalità attraverso le quali l'interessato viene messo a conoscenza di come può esercitare i suoi diritti;
2. art. 13 e 14: informazioni che devono essere fornite all'interessato e le relative modalità;
3. art. 15: diritti di accesso dell'interessato alla conoscenza di quali dati che a lui si riferiscono sono in possesso del Titolare, i relativi trattamenti e quanto a questi è correlato in termini di misure di sicurezza;
4. art. 16: diritto di rettifica;
5. art. 17: diritto alla cancellazione (oblio);
6. art.18: diritto di limitazione del trattamento;
7. art.19: obbligo di notifica da parte del Titolare all'interessato in caso di rettifica, cancellazione, limitazioni;
8. art. 20: portabilità dei dati, la possibilità cioè, di richiedere e ottenere su adeguato supporto tecnologico e in formati elaborabili, i dati detenuti dal Titolare;
9. art. 21: opposizione al proseguimento di un trattamento;
10. art. 22: l'interessato ha il diritto di non essere sottoposto ad un processo automatizzato che produca effetti giuridici che lo riguardano o che incida sulla sua persona, salvo i casi previsti al comma 2 dello stesso articolo.

I diritti richiamati, a norma dell'art. 23 (C73) e per le motivazioni espresse nello stesso articolo, possono subire delle limitazioni.

In estrema sintesi il processo prevede l'informazione preventiva dell'interessato, la richiesta del consenso dove applicabile, come misure antecedenti l'avvio del trattamento con riguardo ad una persona fisica e il diritto della stessa di poter intervenire, con modalità certe e tempi definiti, nell'ambito dei trattamenti e relativi dati che lo riguardano, sia per acquisirne la conoscenza sia per richiedere eventuali misure fra quelle previste dal regolamento.

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

10. Modello organizzativo da adottare

Come evidenziato, nell'organizzazione Data Protection esistono alcuni ruoli e funzioni chiaramente identificati in capo a determinate istanze organizzative, così come sono chiaramente identificati i processi che sostengono la compliance organizzativa al GDPR.

Ferme restanti le competenze e i vincoli dei diversi soggetti nei rispettivi ruoli, vengono individuate le nuove *strutture di supporto e la loro collocazione organizzativa* per il supporto nella gestione dei processi.

Le competenze e le figure di supporto sono quelle riconducibili all'Ufficio DPO, presso il quale sono dislocati i "Data Protection Specialist".

L'Ufficio DPO di ARPAT è identificato all'interno del Settore SIRA.

Nel seguito si prendono i processi GDPR e per ciascuno di essi si descrivono i compiti nei diversi livelli organizzativi.

10.1 Data Protection by design and by default

Tale processo riguarda la "formazione degli atti" da cui discendono trattamenti di dati personali e la realizzazione di sistemi automatizzati o meno che attuano indirizzi e scelte definiti in tali atti.

Al fine di presidiare il processo di formazione degli atti in modo che sia compliant con il GDPR si procede come segue:

a) si assegna al Settore SIRA (ovvero alla struttura che ha in carico le funzioni di "Responsabile ICT" e "Ufficio DPO") il compito di supportare il Titolare, i Responsabili e gli autorizzati , nel definire, per ogni atto di loro competenza, se è coinvolta o meno la problematica della protezione di dati personali, e se nel caso aggiornare l'atto con quanto necessario ad impostare gli elementi di data protection e seguire l'evoluzione susseguente l'adozione dell'atto stesso.

b) A tal fine il SIRA è:

- punto di riferimento multidisciplinare a supporto del Titolare, del DPO, dei Responsabili di struttura e degli incaricati;
- punto di contatto con gli interessati;
- punto di riferimento organizzativo di supporto alle interlocuzioni con il Garante;
- punto di riferimento organizzativo per la gestione del Dossier data protection.

c) si assicura adeguata formazione in materia di data protection ai proponenti degli atti (Delegati ai trattamenti) e al personale dell'ufficio che ha il compito istituzionale di effettuare il controllo formale sui decreti (Settore Affari generali);

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

d) si attribuisce ai Direttori la responsabilità di predisporre la DPIA (Valutazione d'impatto sulla protezione dei dati di cui all'art. 35 del GDPR) relativa ai trattamenti di competenza, nei casi previsti.

   La DPIA è predisposta con il supporto del Responsabile ICT/ Ufficio DPO e delle strutture di riferimento per il trattamento indicate nel Registro trattamenti ed è approvata dal Titolare.

e) si attribuisce ai Delegati la responsabilità di:

   i. verificare e attestare che gli atti di cui sono proponenti non attivino trattamenti non previsti nel Registro (tenuto conto che sono consentiti: i soli trattamenti elencati nel Registro, nelle modalità indicate nell'informativa, per le categorie di interessati e di dati personali in esso previsti; i soli trasferimenti dei dati a terzi indicati nel Registro; le sole comunicazioni dei dati a terzi indicate nel Registro);

   ii. allegare agli atti che attivano trattamenti con nuovi sistemi informatici:

      - l'informativa relativa al trattamento o documentare le motivazioni per le quali non sia necessaria;
      - la DPIA (Valutazione d'impatto sulla protezione dei dati di cui all'art. 35 del GDPR) o documentare le motivazioni per le quali non sia necessaria;
      - il parere del Responsabile ICT/ Ufficio DPO al fine di verificare la conformità con la normativa su data protection e ICT.

   iii. Indicare, negli atti di cui sono proponenti, se hanno rilevanza per la data protection e, nel caso il proponente sia diverso dal RUP, impegnare il RUP a notificare l'atto, dopo l'approvazione, all'Ufficio DPO per conservazione nel dossier data protection. Per la data protection sono rilevanti le seguenti tipologie di atti:

      - contratti o accordi relativi ad affidamento di trattamenti dati a soggetti esterni (ad esempio attivazione di sistemi informatici o altre attività che prevedono trattamento dati, ove deve essere prevista la nomina del Responsabile esterno);
      - contratti o accordi relativi allo svolgimento di attività insieme a soggetti esterni (ad esempio convenzioni con altri enti pubblici, ove deve essere previsto l'accordo data protection di contitolarietà);
      - attivazione di trattamenti con nuovi sistemi informatici;
      - normativa ICT e trattamenti dati;
      - aggiornamento del Registro trattamenti;
      - DPIA.

   iv. notificare all'Ufficio DPO, per conservazione nel dossier data protection, gli atti adottati che riguardano la data protection:

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

f) si attribuisce all'ufficio che ha il compito istituzionale di effettuare il controllo formale sui decreti (Settore Affari generali) la responsabilità di verificare che i decreti proposti contengano gli elementi e le valutazioni di cui al precedente punto d).

10.1.1 Mantenimento del registro dei trattamenti

L'art. 30 del GDPR (C82) pone in capo al Titolare la responsabilità di tenere un registro delle attività di trattamento, attività svolta dal Direttore tecnico e dal Direttore amministrativo per i trattamenti di competenza.

Per la predisposizione/aggiornamento del Registro si stabilisce quanto segue:

a) di prendere come riferimento per i trattamenti il titolario di archivio (sistema di classificazione dell'archivio di ARPAT, freedocs) in quanto è un sistema usato da anni per classificare i documenti che si producono in Agenzia e quindi anche le attività connesse;

b) di prevedere una prima stesura del Registro e successive revisioni, definendo accorpamenti delle attività, che hanno caratteristiche di omogeneità nei confronti dei soggetti interni che le svolgono;

d) di attribuire la responsabilità di promuovere l'aggiornamento del Registro ai Direttori, in funzione delle competenze loro attribuite dal regolamento organizzativo, d'intesa con il Responsabile ICT/Ufficio DPO.

10.1.2 Valutazione Impatto (DPIA)

La valutazione di impatto rappresenta una componente fondamentale del processo di data protection by design e by default e costituisce un documento aggiuntivo che va ad aggiungersi alla formazione corretta di atti che per natura dei loro contenuti riguardano trattamenti di "dati particolari".

La DPIA è predisposta dal Direttore competente che, per questa attività, si avvale delle strutture di riferimento per quel trattamento e del supporto del Responsabile ICT/ Ufficio DPO (presso il quale sono dislocati i data protection specialist).

Il DPO assicura, a norma dell'art.35 punto 2 e art. 39 lettera c) del GDPR, supporto di consulenza alla redazione delle DPIA.

L'approvazione della DPIA è a cura del Titolare, a norma dell'art. 35 punto 1 del GDPR.

10.2 Accountability

Premesso che:

a) l'attività di accountability a norma del regolamento è in carico al Titolare o suo delegato e quindi in capo ad ogni dirigente, che per questo compito si avvale di strutture centralizzate quali:

- Security Manager;

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

- DPO e Settore SIRA (presso il quale sono concentrati i data protection specialist);

b) l'attività di monitoraggio, per assicurare il rispetto dei principi di controllo, con particolare attenzione al principio della separazione delle funzioni è in carico a:

   a) security manager (monitoraggio tecnico della componente ICT);

   b) DPO e Settore SIRA (monitoraggio della componente data protection);

   c) Settore Pianificazione Controllo e Sistemi di Gestione (monitoraggio ICT e data protection nell'ambito del piano annuale della qualità dell'Agenzia (PAQ), ove sono definiti obiettivi di monitoraggio concordati con security manager, DPO, Ufficio DPO o definiti di sua iniziativa).

In tale contesto il ruolo delle direzioni e dei singoli dirigenti è quello di offrire il massimo supporto all'Ufficio DPO e al DPO stesso in tutte quelle fasi in cui possa venir richiesto dal Garante o dagli interessati, informazioni in merito ai processi messi in atto al fine di garantire il pieno rispetto del GDPR.

10.3 Monitoraggio, controllo misure di sicurezza e gestione degli incidenti

Tale processo è gestito centralmente dalle strutture del Security Manager, del DPO, dell'Ufficio DPO e dalle strutture tecniche di riferimento, per la gestione dei sistemi o degli archivi.

10.4 Informazione e Garanzia dei diritti degli interessati

Si delegano:

a) Direttori: alla predisposizione delle informative per gli interessati relativamente ai trattamenti di competenza. L'informativa è predisposta con il supporto delle strutture competenti per i singoli trattamenti, individuate nel Registro trattamenti e con il supporto consulenziale dell'Ufficio DPO.

b) Dirigenti: alla informazione agli interessati, con il supporto dell'Ufficio DPO;

c) Ufficio DPO: alla attuazione del processo per la garanzia dei diritti dell'interessato e alla definizione della modulistica standard per le informative.

11. Rapporti fra DPO e il Titolare

Il DPO, nel caso rilevasse criticità di ordine generale in merito all'obiettivo di garantire la compliance al GDPR, provvede a segnalare al Titolare le criticità organizzative e tecniche o le eventuali violazioni accertate, che possano comportare l'insorgere di una responsabilità in capo all'Ente per non conformità al GDPR, anche ai fini degli opportuni provvedimenti.

Tali comunicazioni, su una base periodica e di necessità, riguardano ogni aspetto che il DPO ritiene di sottoporre al Titolare, ai fini della conformità al GDPR, tra cui si citano a titolo esemplificativo:

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

a) informazioni sul livello di adeguatezza della sicurezza e della capacità di prevenzione di trattamenti in violazione del Regolamento,

b) evidenze di ipotesi di trattamento a “rischio elevato” ,

c) istanze da presentare all’Autorità di controllo,

d) ispezioni da parte dell’Autorità di controllo,

e) criticità inerente la protezione dei dati personali, anche in relazione ad eventuali segnalazioni esterne o interne ricevute dall’Ente.

12. Rapporto fra processi GDPR e Procedimenti amministrativo-decisionali

Nella precedente sezione sono stati esaminati i processi che il GDPR prevede nell'ambito di una organizzazione compliant, coerente ai suoi principi e ai suoi dettati. In questa sezione delle linee guida, vengono individuate le misure necessarie a rendere tali processi intrinsecamente connessi con i procedimenti amministrativi dell'ente al fine di non creare percorsi paralleli di difficile gestione e possibili disallineamenti fra i processi decisionali e attuativi e quelli di valutazione dei rischi in caso di trattamenti di dati personali.

12.1 Data Protection by design and by default

Come richiesto dal processo di Data Protection by Design, il tema della protezione dei dati personali deve essere preso in considerazione fin dal nascere di una nuova iniziativa.

Pertanto in ogni atto dell'amministrazione sia esso un decreto o un altro atto, occorre che sia data evidenza se negli effetti dell'atto vengono coinvolti processi e trattamenti relativi a dati personali e, nel caso, occorre coinvolgere l’Ufficio DPO per la creazione o aggiornamento del dossier data protection.

Al fine di dare supporto a tale procedimento sarà opportunamente modificato il Disciplinare ICT e trattamenti dati. Occorre inoltre:

- che sia modificata la procedura di gestione degli atti secondo criteri che saranno definiti nel Disciplinare ICT e trattamenti dati, in modo da inserire a cura del dirigente se quell'atto ha rilevanza in materia di dati personali, e se sì alcuni dati descrittivi in termini di trattamenti, liceità degli stessi, caratteristiche dei dati stessi e numerosità e tipologia degli interessati, l'identificativo del dossier se esistente oppure la creazione di uno nuovo. Nel caso di atti che si riferiscono a dossier già attivati si dovrà rendere conto del fatto che il dossier è stato aggiornato con i documenti previsti nel processo di Data Protection by Design,
- che sia realizzato all'interno del sistema documentale il Dossier Data Protection per i diversi processi che verranno attivati, secondo criteri che saranno definiti nel Disciplinare ICT e trattamenti dati

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

Si ricorda che la gestione del Dossier è finalizzata a rendere agevole la attività di accountability in quanto terrà traccia di tutti gli adempimenti fatti, di tutte le scelte fatte e delle relative motivazioni.

L'Ufficio DPO:

- procede alla verifica preventiva della rispondenza al GDPR delle proposte di decreto che attivino trattamenti con nuovi sistemi automatizzati, per eventuale aggiornamento dell'atto con quanto necessario ad impostare gli elementi di data protection;
- effettua un monitoraggio a campione sugli atti.

12.1.1 Mantenimento del registro dei trattamenti

La gestione del registro dei trattamenti è assicurata da Direttori tecnico, Direttore Amministrativo e Responsabili di struttura per i trattamenti di loro competenza.

I Delegati (Direttore tecnico, Direttore Amministrativo e Responsabili di struttura)

a) al momento della predisposizione di atti amministrativi individuano se quell'atto prefigura o interviene in processi che prevedono il trattamento di dati personali, nonché se è necessario prevedere la stipula di appositi *data protection agreement* in base alle regole dedicate ai rapporti DP con terze parti;

b) se ritenuto necessario, richiedono il supporto i Data Protection Specialist e consultano il DPO per tutte le questioni riguardanti la individuazione dei trattamenti, delle loro caratteristiche e delle azioni da porre in essere per la loro corretta gestione nel tempo;

Per le modalità di mantenimento del Registro si rimanda al para. 10.1., ivi compresa l'esigenza di procedere alla formulazione di una DPIA.

12.1.2 Richiesta pareri, formulazione e gestione della DPIA

I Direttori e i Dirigenti:

a) attraverso il supporto dei Data Protection Specialist e per mezzo di un futuro applicativo dedicato "Richiesta Pareri", possono indirizzare all'attenzione del DPO la richiesta di pareri formali in merito a questioni riguardanti la protezione dei dati;

b) collaborano alla predisposizione della DPIA;

c) richiedono il parere del DPO a chiusura della DPIA e la inviano all'Ufficio DPO per inserimento nel Dossier Data Protection.

12.2 Monitoraggio Organizzativo e Accountability

Come evidenziato nelle precedenti sezioni, elemento fondamentale per la compliance al GDPR è mettere in atto meccanismi organizzativi che rendano l'attività di protezione del dato, una attività, un pensiero corrente che accompagni l'operato di ogni dipendente con particolare riferimento all'azione dirigenziale che si assume la responsabilità derivante dal suo ruolo di

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

delegato del Titolare. Al tempo stesso i dirigenti devono essere messi in grado dall'amministrazione di poter svolgere con efficienza ed efficacia la loro responsabilità. In questa ottica Il DPO, con l'Ufficio DPO, provvederà a redigere apposita relazione sull'adeguatezza dell'organizzazione ai compiti derivanti dall'attuazione del GDPR.

I Dirigenti devono:

a) in fase di monitoraggio da parte dell'Ufficio DPO, fornire la massima collaborazione tesa ad evidenziare problemi ed ad individuare soluzioni,

b) in fase di segnalazioni da parte di interessati provvedere, con il supporto eventuale del DPO o del suo ufficio, a mettere in atto misure adeguate a rendere conto delle situazioni oggetto di segnalazione ed eventualmente a mettere in atto misure idonee alla risoluzione dei problemi evidenziati

c) in fase di ispezione o indagine del garante offrire tutta la collaborazione possibile.

12.3 Monitoraggio tecnologico, controllo misure di sicurezza e gestione degli incidenti

Il Monitoraggio tecnologico è in carico al Security Manager che provvede:

a) alla redazione e attuazione di un piano per le verifiche sulle misure di sicurezza messe in atto dai dirigenti responsabili dei sistemi e delle applicazioni IT o di fornitori esterni;

b) alla verifica della rispondenza delle misure di sicurezza in essere alle linee guida emesse dal DPO;

c) alla relazione periodica sulle misure di sicurezza adottate evidenziando punti di criticità e proponendo remediation plan.

La gestione degli incidenti è in carico al Security Manager che:

a) registra l'incidente;

b) avvisa il Titolare dei trattamenti coinvolti nell'incidente;

c) provvede ad una valutazione dell'incidente in termini di gravità con la collaborazione del dirigente/i coinvolto/i nel trattamento/i;

d) provvede a relazionare al DPO per la decisione relativa alla segnalazione al Garante, alla segnalazione agli interessati, alla segnalazione all'autorità giudiziaria se trattasi di atto potenzialmente doloso.

I dirigenti responsabili per ambiti di competenza alla sicurezza IT o titolari di contratti in essere per la fornitura di servizi IT debbono assicurare:

a) tutte le condizioni idonee, di collaborazione e contrattuali verso fornitori (individuati come Responsabili) al fine di consentire un efficiente ed agevole lavoro del Security Manager;

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

b) l'attuazione del remediation plan indicato dal Security Manager nei tempi indicati nello stesso;

c) fornire il supporto in caso di segnalazioni di incidenti al fine di comprendere la gravità degli stessi;

d) la tempestiva segnalazione al security manager della evidenza di incidenti che possono aver coinvolto dati personali.

13. Garanzia dei diritti degli interessati

Il Direttore tecnico, il Direttore Amministrativo e i Responsabili di Struttura, al momento della definizione del trattamento identificano e mettono in atto le procedure idonee a fornire adeguata informativa agli interessati. Per la corretta individuazione dei contenuti e della forma dell'informativa il dirigente si avvale dei fac-simili messi a disposizione dall'Ufficio DPO.

Gli interessati tramite i punti di contatto pubblicati per l'interlocuzione con il Titolare e il DPO e attraverso specifico modulo effettuano la richiesta, il DPO provvede alla risposta e a dare indicazioni alle strutture competenti al fine di dare fattiva e tempestiva risposta alle richieste.

Per tale obiettivo, occorre dare attuazione alla previsione di istituire il "fascicolo del cittadino" come collezione delle banche dati o archivi nelle quali sono presenti i relativi dati personali.

14. Attribuzione compiti e responsabilità

L’attribuzione dei compiti e delle responsabilità per l’applicazione del GDPR in ARPAT è descritta nel Disciplinare ICT e trattamenti di ARPAT, che sarà aggiornato conformemente al modello organizzativo definito nel presente atto.

tel. 055.32061 - PEC: arpat.protocollo@postacert.toscana.it - p.iva 04686190481 - www.arpat.toscana.it - urp@arpat.toscana.it

Data Protection Policy
Linee guida per l'attuazione dei processi GDPR
Regione Toscana

REGIONE TOSCANA

Documento redatto da

Approvato con :

Data Protection Policy
Linee Guida Processi GDPR
Indice

1 Scopo del Documento

Questo documento ha come obiettivo di illustrare la "Data Protection Policy" della Regione Toscana in ottemperanza a quanto stabilito dal regolamento UE 2016/679, (GDPR). La Data Protection Policy è costituita da linee guida in merito alla revisione dei processi e dei comportamenti organizzativi nel rispetto dei principi fondamentali della Data Protection by Design e by Default, dell'Accountability a tutela dei diritti e delle libertà delle persone, in riferimento a tutti i trattamenti che coinvolgono dati personali.

2 Premessa

La presente introduzione è necessaria al fine di inquadrare sotto un profilo contestuale il Regolamento Europeo nr. 2016/679 (General Data Protection Regulation meglio noto come GDPR), entrato in vigore il 24 maggio 2016 che ha trovato piena attuazione a partire dal 25 maggio 2018, che uniforma ed armonizza le legislazioni dei Paesi Europei con riguardo alla materia di protezione dei dati personali.
L'esigenza di una rivisitazione della normativa in materia di protezione dei dati personali si apprezza in relazione al mutato contesto politico, economico e sociale di riferimento del tutto differente rispetto a quello degli anni 90, periodo nel quale l'impatto e la cultura del dato non era così centrale come invece lo è oggi. Ciò è dipeso dallo sviluppo repentino delle moderne tecnologie (in primis mobile devices, smartphone, tablet, social network, ecc.; in seconda battuta strumenti IOT (Internet of things), sistemi di Data Analytics e Big Data, Business Intelligence, ecc.) nemmeno immaginabile negli anni che chiudevano il secolo scorso, che hanno attribuito al dato personale un vero e proprio valore economico.
Accanto a questa constatazione di tipo "sociologica" va da sé che il programma di integrazione europeo che vede come base di partenza la creazione di un mercato unico europeo, da realizzarsi inizialmente attraverso la libera circolazione di persone, servizi e merci, non possa non tenere in considerazione anche ~~del~~la libera circolazione del "dato personale" così come puntualmente sottolineato dai "considerando" del Regolamento fino anche alla maggiore rilevanza di questa libertà rispetto alla tutela del dato in sé come diritto soggettivo (considerando nr. 4 del GDPR).
A seguito di questa breve introduzione storica/sociologica ed avviando la riflessione sul terreno giuridico, in prima battuta preme precisare che la scelta di tipologia di intervento del legislatore Europeo risulta alquanto significativa nella misura in cui, con la scelta di un Regolamento, non viene lasciata agli Stati membri alcuna possibilità di intervento (se non in termini di adozione di provvedimenti volti ad armonizzare la normativa nazionale) stante la piena applicabilità del Regolamento a dispetto della presenza, come successo invece in passato in materia di protezione di dati personali, di direttiva europea (95/46) che necessitava di un atto di recepimento (Dlgs. 196/2003, meglio noto come codice della privacy).
In riferimento invece ai contenuti del regolamento europeo, si sottolinea come l'approccio che propone il Regolamento sia del tutto differente rispetto a quello proposto dal codice privacy nazionale.
Principio fondamentale che impernia l'intera normativa è infatti quello di **accountability** (la capacità di rendere conto delle azioni) il quale richiede, una responsabilizzazione dei soggetti coinvolti in materia di protezione di dati personali. Questi infatti secondo il dettato normativo non dovranno più ragionare in termini di mero adempimento alla norma di riferimento, come invece accaduto fino ad oggi con riferimento ai dettami del codice della privacy.
In tal senso il principio di accountability deve essere letto sotto un duplice profilo: esso non solo è il principio che ispira l'adeguamento/l'adempimento degli enti alla normativa europea, ma è anche il punto di partenza per **dimostrare** la compliance (il rispetto, l'aderenza)

dell'ente/organizzazione alla norma europea. In tale ottica, il principio in tema informa l'intero arco di attività – compresi gli audit - svolte dal Titolare per gestire qualsiasi "proprio" trattamento, tanto sotto il profilo tecnico/tecnologico quanto sotto il profilo organizzativo e documentale.
Ciò significa che un ente/organizzazione può articolare i propri comportamenti per il rispetto dei principi del regolamento come meglio crede per raggiungere in maniera sostenibile l'ottimale configurazione dei trattamenti, unitamente alla migliore protezione possibile dei dati personali che tratta, avendo tuttavia cura di indicare in apposito documento le ragioni in forza delle quali si effettuano tali scelte. L'assenza di un modello di adeguamento univoco "imposto" dal legislatore, che discende dall'impostazione del documento (principo della accountability), di fatto costringe il titolare e il responsabile – ove previsto - ad effettuare una attenta analisi dei trattamenti e dei rischi connessi, dei costi e dei benefici e portare le giustificazioni a supporto delle decisioni prese (DPIA).
Sotto il profilo dei soggetti attivi e protagonisti, in questo nuovo quadro, tra le varie innovazioni previste dal GDPR va segnalata l'introduzione della figura del **Data Protection Officer – DPO** (obbligatorio, tra l'altro, per tutti gli enti pubblici) il quale si andrà a configurare da un lato come consulente per i Titolari e i Responsabili dei trattamenti, attraverso una continua verifica della compliance dell'organizzazione/ente rispetto ai dettami del GDPR, ma anche come punto di riferimento per i soggetti interessati e l'Autorità di controllo, rappresentando per questi ultimi il referente dell'organizzazione con il quale interfacciarsi in materia di protezione dei dati personali.
In conclusione, come già emerso dalla disamina condotta, a mutare è l'atteggiamento della normativa rispetto alla tematica della protezione dei dati personali, esso infatti impone una riflessione preventiva rispetto alla materia de qua, che porta quindi ad adattare la propria organizzazione in base alle opportunità che si intendono cogliere, lasciando non solo ampi spazi di autonomia ai soggetti Titolari/Responsabili ma anche abbandonando quell'approccio di mero adempimento richiesto dalla normativa. In sintesi, non è sufficiente avere "le carte a posto".

3 Data Protection Policy

La Data Protection Policy si muove su due macro linee, sull'adeguamento dell'organizzazione e sulla messa in atto di nuovi processi. Pertanto essa è composta da una linea guida sull'organizzazione approvata con delibera di Giunta nr. 521 del 23 April2 2019 e dalle presenti linee guida per l'attuazione dei processi GDPR. Approvati con decerto dorgenziale..

La ***linea guida sull'Organizzazione*** di cui alla delibera di Giunta regionale della Toscana, descrive come l'organizzazione precedente alla entrata in vigore del GDPR, viene a modificarsi sulla base delle nuove figure, strutture organizzative e relative attribuzione di compiti e responsabilità, previste in maniera esplicita o implicita dallo stesso GDPR.

I processi derivanti dall'attuazione del GDPR, che devono essere messi in atto dall'organizzazione sono:

a) ***Processo Data Protection by Design/by Default:*** finalizzato ad introdurre il tema della data protection fin dalle prime fasi di progettazione di tutte le soluzione che prevedano il trattamento di dati personali e questo in collegamento con la produzione degli atti amministrativi relativi a proposte di leggi, regolamenti, convenzioni, bandi, contratti, ecc.. All'interno di questo processo hanno particolare rilevanza due sotto-processi di cui uno relativo alla *gestione del registro dei trattamenti* e l'altro alla *valutazione di impatto della data protection (DPIA),*

b) ***Processo per le garanzie e le tutele dei diritti degli interessati:*** finalizzato a mettere in atto quelle azioni e quei servizi di rapporto con le persone, per informarle in merito alle finalità ed utilizzo dei loro dati personali e per rispondere alle loro istanze, previste come diritti dell'interessato nell'ambito del GDPR,

c) ***Processo di gestione degli incidenti***: finalizzato alla registrazione di incidenti di sicurezza, alla loro valutazione in termini di danni potenziali o reali arrecati e relative procedure di comunicazione e denuncia previste dal GDPR,

d) ***Processo di Accountability***: finalizzato a poter rendere conto alle persone, al garante nazionale, all'autorità giudiziaria in merito: al processo di adeguamento (compliance) organizzativo, all'uso appropriato di dati personali, alla valutazione dei rischi e alla adeguatezza delle misure messe in atto per evitare o ridurre i danni conseguenti dell'avverarsi di minacce.

Ognuno di questi processi produce degli output , dei documenti ,che costituiscono la rappresentazione e testimonianza di quanto viene fatto in termini di Data Protection.
Nella tabella seguente sono riportati i principali processi e i principali output.

Processi	***Output***
Processo Data Protection by Design/ by Default, nell'ambito del quale si evidenziano i seguenti sottoprocessi: . Gestione dei Trattamenti . Data Protection Impact Assessment . Gestione Dossier Data Protection	 Registro Trattamenti DPIA Dossier Data Protection
Processo Garanzia dei diritti degli interessati	Fascicolo dell'interessato, comunicazioni agli interessati
Processo Gestione incidenti e notifiche	Registro degli incidenti, Notifiche
Processo di Accountability	Compliance organizzativa Compliance di processo Accountability su processo

Descrizione degli output

Registro dei trattamenti: contiene per ogni struttura, e quindi per ogni dirigente che opera come delegato del Titolare, la descrizione dei trattamenti di dati personali, le misure di sicurezza adottate, il personale autorizzato a quel trattamento,
DPIA: Data protection impact analisys, che descrive in relazione ad un trattamento o gruppi omogenei di trattamenti, i rischi, le minacce e le misure di sicurezza ritenute adeguate a garantire diritti e delle libertà delle persone,
Dossier Data Protection: contiene tutti i documenti relativi alla messa in esercizio di un nuovo processo o alla rivisitazione di uno esistente e alla sua gestione. Il dossier pertanto oltre agli atti e progetti, contiene i riferimenti ai risultati delle DPIA, ai trattamenti che lo compongono, agli incidenti occorsi, alle notifiche effettuate ecc..

Registro degli incidenti: Contiene la registrazione di tutti gli incidenti a prescindere dalla loro rilevanza;
Notifiche: si riferiscono agli atti di comunicazione al Garante nazionale, all'autorità giudiziaria o agli stessi interessati in merito agli incidenti occorsi e che a norma del GDPR devono essere notificati,
Fascicolo dell'interessato: è composto dagli identificativi dell'interessato e dai riferimenti a tutte le basi di dati dove sono contenuti dati personali che a lui si riferiscono;
Informativa agli interessati: sono i modelli di informative che devono essere rilasciati obbligatoriamente per informare le persone perché vengono richiesti tali dati, come saranno trattati e quali sono i contatti da utilizzare per l'esercizio dei loro diritti sanciti dal GDPR,
Compliance organizzativa: livello di adesione dell'organizzazione reale al modello descritto nelle linee guida,
Compliance di processo: livello di adesione dei processi e dei procedimenti, nonché dei comportamenti al modello descritto nelle linee guida,
Accountability su processo: descrizione di quanto messo in atto, in relazione ad un processo di gestione di dati personali, al fine di ridurre i rischi e relativi danni per l'interessato

4 Documentazione

I documenti che descrivono, in termini di linee guida, la Data Protection Policy di Regione Toscana, oltre alla revisione del modello organizzativo di cui alla DGR, hanno la seguente organizzazione

1) La carta dei servizi dell' ufficio del DPO verso l'utente interno/esterno
2) linee guida per il processo di DP by design e by default
   a) metodologia di descrizione dei processi
   b) misure di sicurezza
      i) generali
      ii) specifiche
      iii) disciplinari
   c) facsimile accordo fra titolari autonomi (DPA-TT)
   d) facsimile accordo titolare responsabile e sub responsabile (DPA-TR)
   e) facsimile accordo di contitolarità (DPA-CT)
   f) linee guida registro trattamenti
   g) classificazione dei dati/trattamenti ai fini DPIA e misure sicurezza richieste
   h) Linee guida DPIA
   i) Linee guida scrittura bandi/contratti/convenzioni
   j) caratteristiche documentazione tecnica
   k) Dossier Data Protection
3) linee guida Gestione incidenti
   a) Processo Incidenti
   b) Processo di data breach
4) linee guida per processo di accountability
   a) monitoraggio (auditing)
   b) risposta a processi esterni (interessato, garante, autorità giudiziaria)
5) Linee guida processo garanzia diritti dell'interessato
   a) modulistiche di richieste e risposte
   b) informative tipo

Fanno pertanto parte della Data Protection Policy i documenti:

Linee guida Modello Organizzativo di cui alla DGR
Linee guida Processo di Data Protection by Design/Default
Linee guida Processo di Gestione Incidenti
Linee guida Processo Garanzia Diritti degli Interesssati
Linee guida Processo di Accountability

Gli allegati:

Nr.	Titolo	Descrizione
1A	Carta Servizi Ufficio DPO	Modalità e tempi per richiedere ed ottenere informazioni, pareri, accesso ai dati, segnalazioni da parte dell' Ufficio del DPO
A	Analisi dei processi	Indicazione metodologica per l'analisi e la descrizione dei processi
B	Misure di sicurezza	Elencazione delle principali misure di sicurezza da adottare per la protezione di dati personali
C	DPA-TT	Facsimile di data protection agreement per al regolazione dei rapporti data protection fra ***Titolari Autonomi***
D/E	DPA-TR	Facsimile di data protection agreement per al regolazione dei rapporti data protection fra ***Titolari Responsabili e Sub-responsabili***
F	DPA-CTT	Facsimile di data protection agreement per la regolazione dei rapporti data protection fra ***Titolari in regime di Contitolarità***.
G	Linee guida Registro Trattamenti	Descrive modalità e contenuti del registro delle attività di trattamento
H		
I	Linee guida DPIA	Descrive finalità, contenuti e processo di esecuzione di una analisi di impatto in termini di data protection (***D***ata***P***rotection***I***mpact***A***nalisys)
L	Linee guida per al formulazione di Contratti/convenzioni/protocolli di intesa	Descrive la metodologia di analisi di contratti/convenzioni/protocolli di intesa al fine di individuare i ruoli previsti dal GDPR e le relative responsabilità nella gestione delle attività di trattamento
M/N	Linee guida misure di sicurezza	Descrive le modalità applicative delle misure di sicurezza
O	Dossier Data Protection	Descrive finalità, contenuti e processo di formazione ed aggiornamento del dossier data protection,.

Processo Data Protection by Design & by Default

Linee Guida

1 Scopo del documento

Il presente documento descrive e costituisce linee guida in termini di attività e responsabilità, per la conduzione del processo di Data Protection by Design/by Default.

"Data Protection by Design" vuol dire che il tema della Protezione dei Dati deve essere tenuto presente nel momento stesso in cui si progetta una iniziativa di qualsiasi genere che implica il trattamento di Dati Personali.
In ambito pubblico una nuova iniziativa può essere una legge, un regolamento, un atto amministrativo, un atto di organizzazione, un bando, sia esso di gara o per l'erogazione di contributi, campagne di informazione, sviluppo di sistemi informativi, contratti, logistica e controlli di sicurezza, ecc..
Potremmo dire che poco o nulla dell'attività pubblica non richiede di porsi la domanda: quello che sto progettando implica il trattamento di dati personali?
Se la risposta sarà si, allora occorrerà applicare quanto previsto dal GDPR il prima possibile.
Il principio di Data Protection by Design si accompagna con quello di Data Protection by Default, che si basa sull'obiettivo di minimizzare al massimo il rischio di uso non lecito o disattento di dati personali. Tale principio si applica nella definizione di operazioni che tendano a coinvolgere dati personali in maniera non ridondante o amplificata rispetto alle effettive esigenze, stabilendo come standard (di default, per l'appunto) il massimo grado di tutela possibile dei diritti "D.P." dell'interessato.

Per chiarezza espositiva si definiscono i seguenti termini
Processo (process): rappresenta l'insieme di operazioni/azioni, poste in essere anche da persone o soggetti organizzativi diversi (strutture organizzative, enti) ma finalizzate al raggiungimento di uno specifico scopo.
Funzioni: insieme di operazioni/azioni, omogenee per competenze e quindi portate avanti da una singola persona, singola struttura organizzativa o singolo ente finalizzate a supportare uno o più processi
Trattamenti (processing): operazioni/azioni o gruppi di operazioni/azioni applicate a dati personali quali la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
Titolare (controller) del trattamento (processing): la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che determina le finalità e i mezzi per il trattamento
Responsabile (processor) del trattamento: Persona fisica, giuridica, o altra organizzazione che effettua il trattamento (processing) per conto del Titolare (controller)
Interessati (data Subject) persone fisiche i cui dati personali sono coinvolti nel trattamento (processing)

5 Contesto di riferimento

Le presenti linee guida si riferiscono alle fasi di *definizione e attuazione di processi* che coinvolgono il trattamento di Dati Personali.
L'obiettivo delle linee guida è quello di essere di ausilio nelle fasi di definizione di un processo e successiva attuazione al fine di stabilire:

1. Se il processo coinvolge, a qualsiasi titolo, l'uso di dati personali riferiti a persone fisiche,

2. Nel caso positivo ad individuare
    a. Il o i Titolari (se più di uno, i rispettivi ruoli di autonomia o contitolarità)
    b. Il o gli eventuali Responsabili e sub-responsabili
    c. Gli interessati
    d. i trattamenti e le relative caratteristiche (base giuridica, finalità, dati, uffici coinvolti, etc.):
        i. L'esigenza o meno di particolari misure di sicurezza
        ii. L'esigenza o meno di approfondimenti (DPIA)
    e. Come regolare:
        i. la con-titolarità rispetto a trattamenti
        ii. Il rapporto fra titolari all'interno di un processo
        iii. Il rapporto fra titolare e responsabile nell'ambito di trattamenti
        iv. Il rapporto fra titolare e interessati
3. Nel caso negativo non si applica il GDPR.

Gli atti attraverso i quali si definiscono processi e per i quali occorre applicare le presenti linee guida qualora siano di nuova istituzione o che si preveda una sostanziale modifica in particolare per quanto attiene il trattamento di dati personali, sono:

- Proposte di leggi regionali
- Regolamenti
- Delibere
- Decreti
- Bandi, contratti o convenzioni di affidamento servizi
- Sviluppo di nuovi sistemi informativi
- Sviluppo di APPS, e di qualsiasi altro sistema di registrazione e gestione di dati personali.

6 Metodologia

La metodologia da seguire al fine di realizzare comportamenti coerenti e rispettosi del GDPR, con particolare riferimento a quanto previsto all'art. 25, in tutti gli ambiti di applicazione delle presenti linee guida è tesa a rilevare, in fase preliminare, le esigenze in termini di protezione dei dati in modo che possano essere chiaramente e univocamente individuate le diverse figure (previste dal GDPR) e relative responsabilità, e previste le misure di sicurezze idonee e commisurate al rischio.
Questo richiede che negli ambiti di applicazione delle presenti linee guida, venga effettuata una analisi preventiva e sulla base di questa adottate le misure ritenute più appropriate atte a garantire una gestione del dato personale in modo conforme al regolamento europeo.
Analisi preventiva che deve necessariamente partire dalla individuazione del processo che si intende andare a realizzare.

7 Analisi preliminare

L'analisi preliminare si compone di due aspetti, l'analisi di processo e l'individuazione dei soggetti coinvolti nel processo e del loro ruolo in termini di GDPR.

a) Analisi di processo

Il processo deve essere descritto, con la granularità adeguata al tipo di atto, in termini di:
1. Obiettivo
2. La categoria dei soggetti interessati
3. Soggetti coinvolti
4. Attività svolte da ciascun soggetto
5. Dati o tipologia trattati.

Il processo deve essere descritto con i formalismi di cui **all'Allegato A**

b) Individuazione delle figure (art. 24 – 43 GDPR)

Tale individuazione si compone di due fasi a seconda della definizione degli obiettivi da realizzare

Fase 1

Sulla base della descrizione del processo, si analizzano gli interessati e i soggetti coinvolti, al fine di determinare a quale titolo vengano svolte le attività che compongono il processo da parte dei diversi soggetti.

1. Si individuano le tipologie di dati trattati, gli interessati coinvolti nel processo come categorie di soggetti e la loro numerosità ipotizzata. Questo servirà a determinare se trattasi o meno di trattamento che interessa una larga scala di persone.
2. Qualora esista una norma di riferimento che individua il soggetto come preposto allo svolgimento di quelle attività, lo stesso viene individuato, a norma del GDPR, come titolare per le attività da lui svolte direttamente o indirettamente.
   Qualora non esista alcuna norma di riferimento, occorre che il Titolare venga esplicitamente individuato nell'atto, in riferimento al trattamento o insiemi di trattamenti derivanti dalle attività facenti parti del processo o segmento del processo in cui il soggetto è coinvolto.
3. Qualora un soggetto non possa essere individuato come titolare, occorre individuare per conto di chi svolge le attività componenti il processo o segmento del processo in cui è coinvolto. Il soggetto per il quale svolge le attività può essere un soggetto "Titolare" oppure un soggetto "Responsabile".
   Nel primo caso quel soggetto si configura come Responsabile nel secondo caso come sub responsabile.
4. Qualora più titolari operino all'interno del processo con le stesse finalità e gli stessi mezzi si configura una situazione di contitolarità.
   Maggiore dettaglio per l'individuazione dei ruoli GDPR nel caso di instaurazione dei rapporti attraverso procedure di gara, contratti, convenzioni o protocolli di intesa viene fornito **Allegato L**

Fase 2

A valle della individuazione delle diverse figure e dei rispettivi ruoli e responsabilità alla luce del GDPR occorre procedere:

a) Alla individuazione dei trattamenti e delle tipologie di dati trattati (art. 5-11 e art.12-23 GDPR)
   1. Sulla base delle attività evidenziate nella descrizione del processo per i diversi soggetti si elencano i trattamenti secondo quanto descritto nelle linee guida sulla costituzione e gestione del registro dei trattamenti, **Allegato G,**

2. Sulla base dei trattamenti si individuano le classi dei dati e il loro livello di sensibilità (comuni, particolari, giudiziari), gli obblighi in termini di produzione di informativa e consenso tenendo presente non solo il dato in sé ma anche la riconducibilità alla persona fisica secondo lo schema in **Allegato H**

b) Alla formalizzazione dei seguenti rapporti al fine di definire il quadro delle responsabilità per il raggiungimento dell'obiettivo dell'intero processo.

1. Per ogni Titolare del trattamento, visto quest'ultimo, come segmento di un processo più generale, e sulla base delle caratteristiche dei dati trattati, occorre siano definite le misure di sicurezza tecnica organizzativa adottate come descritto in **Allegato B**
2. In caso di compresenza di più titolari per segmenti diversi del processo occorre sia stipulato fra i titolari atto convenzionale (Data Protection Agreement DPA) nel quale si chiariscano i ruoli e le misure di sicurezza ai fini dello scambio di dati fra titolari **Allegato C**
3. In caso di rapporto di un titolare con un responsabile occorre siano definiti attraverso apposito DPA, le misure di sicurezza adottate, i sistemi di monitoraggio e controllo, la gestione dei data breach, ecc., occorre considerare inoltre la presenza o meno di uno o più sub-responsabili **Allegato D/E**
4. Nel caso di contitolarità occorre sia redatto DPA nell'ambito del quale siano chiariti i rispetti ruoli e funzioni assicurate **Allegato F**

Per ***Data Protection Agreement***, **DPA**, si intende un accordo separato fra le parti oppure un articolato specifico inserito all'interno di contratti, convenzioni, protocolli di intesa, che regoal i relativi impegni e responsabilità, in merito alla tematica della protezione dei dati in conformità con il GDPR. Il DPA prevede format differenti per i diversi rapporti di responsabilità che si vengono a realizzare fra i soggetti contraenti in virtù del ruolo che vengono a svolgere a norma del GDPR.
Avremo pertanto un format diverso e comunque da personalizzare sulla base delle effettive attività svolte, per regolare i rapporti fra:

a. Titolare e Responsabile
b. Responsabile e sub-responsabile
c. Titolari Autonomi
d. Titolari in Co-titolarità, (Contitolari)

8 Macro Progettazione della soluzione

Sulla base dell'analisi preliminare, si procede alla individuazione della soluzione finalizzata alla realizzazione del processo con particolare riferimento ad individuarne le modalità (interne, esterne, digitali, non digitali,..) e le procedure (convenzioni, bandi di gara, affidamenti, contratti, ecc..) secondo i seguenti passi

1. Conferma, rivisitazione, completamento, aggiornamento dell'analisi preliminare o stesura qualora non sia stata fatta nelle fasi precedenti alla progettazione della soluzione. Questo in quanto l'analisi preliminare sarà stata fatta a livelli di dettaglio diversi rispetto all'atto a cui si riferisce. Ad esempio:

- *proposta di legge* sarà sufficiente l'analisi di processo e opzionale l'individuazione delle figure fase 1,

- *regolamento* dovranno essere presenti sia l'analisi del processo sia l'identificazione delle figure fase 1,
- *delibera attuativa* dovranno obbligatoriamente essere presenti l'analisi di processo, l'individuazione delle figure di cui alla fase 1, gli schemi degli atti convenzionali o altro che legano i rapporti fra soggetti istituzionali (rapporto fra titolari, contitolarità, ecc..)
- *decreto attuativo* l'analisi di processo, la individuazione delle figure, l'approvazione di atti convenzionali, bandi gara, contratti, ecc.. che si conformino, a seconda dei casi, con le indicazioni delle presenti linee guida.

2. Sulla base dell'analisi preliminare svolta e del suo aggiornamento si procede alla progettazione della soluzione che può coinvolgere soluzioni IT o meno. In ogni caso il sistema che si va a realizzare deve contenere una relazione dettagliata in merito all'analisi dei rischi, allo svolgimento o meno di una DPIA motivando la scelta. Al fine della determinazione della obbligatorietà o meno di una DPIA e per il suo svolgimento si segue quanto previsto in **Allegato I,**

3. Si procede se necessario alla formalizzazione, dei bandi e dei successivi contratti, o di convenzioni/protocolli di intesa secondo quanto previsto in **Allegato L**

9 Progettazione di dettaglio

Sulla base della macro progettazione viene dato seguito alle procedure amministrative (delibere/decreti) che consentono di procedere alla realizzazione tecnica organizzativa della soluzione. A valle di queste si procede alla progettazione di dettaglio che deve essere integrata con:

1. Valutazione, aggiornamento, integrazione di quanto prodotto nelle fasi precedenti con particolare riferimento all'analisi dei rischi e indicazioni delle misure di sicurezza messe in atto nella progettazione di dettaglio e seguite nella successiva fase di realizzazione e della loro aderenza a quanto previsto nella eventuale DPIA aggiornandola, **Allegato M,**
2. Documentazione degli asset coinvolti (banche dati, infrastrutture di rete, application server, applicazioni, Identity Access Method, …) e delle misure di sicurezza adottate (art. 32 GDPR), **Allegato N,**
3. Descrizione dei dati personali presenti nelle diverse banche coinvolte nella esecuzione del processo,
4. Descrizione di dettaglio dei trattamenti dati derivanti dalla soluzione realizzativa del processo,
5. Descrizione di dettaglio degli obblighi derivanti dalla compresenza di titolari, di contitolarità, di rapporti con responsabili e sub responsabili nella trasmissione, condivisione e gestione di dati personali,
6. Descrizione dell'assolvimento delle procedure di eventuale richiesta di parere al garante, di realizzazione o non realizzazione della DPIA,
7. Descrizione delle modalità di informativa all'interessato,
8. Descrizione delle misure tecniche organizzative al fine di mantenere adeguate le misure di sicurezza al variare delle minacce e dell'evoluzione tecnologica,
9. Descrizione delle modalità e delle garanzie per garantire al controllore della sicurezza, Security Manager di poter svolgere con efficacia il proprio lavoro,

Il processo di Data Protection by Design nella sua fase iniziale, qualunque essa sia fra quelle descritte, apre (crea) il "Dossier Data Protection" di cui allo schema **Allegato O,** e sarà aggiornato puntualmente da tutte quelle successive.

10 Verifica della progettazione di dettaglio

Al fine della accountability (art.24-31 GDPR) occorre procedere alla verifica della completezza e della adeguatezza del "Dossier Data Protection" allegato alla progettazione"

1. Viene valutata la soluzione organizzativa
2. Vengono valutate le misure di sicurezza adottate in relazione ai rischi
3. Viene verificato che i trattamenti e quanto a loro collegato siano stati correttamente inseriti nel registro dei trattamenti

11 Messa in esercizio della soluzione

Preliminarmente alla messa in esercizio della soluzione occorre sia stata effettuata con esito positivo l'attività di verifica. Qualora per motivi di urgenza sia necessaria la messa in esercizio della soluzione questo può avvenire con decisione scritta e motivata da parte del titolare o suo delegato, e comunque quando trattasi di processi o trattamenti che non coinvolgono dati personali particolari. Durante l'esercizio delle nuove procedure sia che esse siano digitali o meno, dovrà essere mantenuto aggiornato il Dossier Data Protection che conterrà anche gli incidenti e le eventuali comunicazioni al garante e agli interessati.

12 Dossier Data Protection

Il dossier mantiene traccia nel tempo del processo di costruzione di una soluzione ad un bisogno e la storia della sua gestione **(Allegato O)**.
Il dossier si forma attraverso un processo continuo, viene formalizzato nella fase di macro-progettazione sulla base di precedenti documenti e ne viene gestito il ciclo di vita dal responsabile del sistema informativo/organizzazione.

13 Conduzione del processo di Data Protection by Design

Le ***figure e i ruoli*** del processo di Data Protection by Design, che accompagna la progettazione e la messa in esercizio di soluzioni digitali o meno, nell'ambito delle competenze della Regione o di altri enti sono:
Il titolare e suoi delegati operano anche attraverso i loro referenti o quelli della Direzione di appartenenza a seconda del livello di progettazione,
Il responsabile dei sistemi informativi: la struttura dirigenziale deputata a tradurre l'ipotesi di soluzione in macro progettazione e progettazione di dettaglio e successivamente alla messa in esercizio di quanto progettato,
Il responsabile sicurezza delle infrastrutture: la struttura dirigenziale deputata a tradurre, in collaborazione con il responsabile dei sistemi informativi, l'ipotesi di soluzione in macro progettazione e progettazione di dettaglio in riferimento ai servizi infrastrutturali quali sistemi, reti, middleware, ecc..

Il Security IT Manager/Resp. Archivi: il responsabile della struttura deputata a verificare, sia in fase di progettazione sia durante la vita della soluzione, l'adeguatezza delle misure di sicurezza adottate.
Ufficio del DPO: struttura di supporto e consulenza del titolare e sui delegati con un compito specifico di verifica e rilascio di parere non vincolante del dossier data protection che descrive la soluzione in via di adozione, alla luce del GDPR.

Nella tabella riportata di descrizione del processo si incrociano le diverse figure organizzative con le attività dove con il prefisso **"I:"** si individuano gli elementi in ingresso e con **"O:"** si indica l'output attraverso gli elementi prodotti.
Per attività di consulenza si intende indicare che sarebbe opportuno che la relativa struttura venisse consultata o informata anche nelle fase propedeutiche alla realizzazione di soluzioni, in modo da garantire un processo di accompagnamento di attività che ancora non hanno raggiunto la formalizzazione dei trattamenti.

14 Diagramma del processo : Data Protection by Design

Fase del processo	*Titolare/Referenti del titolare*	*Titolare/Referenti della Direzione*	*Security IT manager Resp. archivio*	*Ufficio del DPO*	*Resp Sistema Inf. Resp. sic. infrastr.*
Analisi Preliminare: analisi del processo	I: Bisogni O: obiettivi	I: obiettivi O:descrizione processo			Consulenza
Analisi preliminare: individuazione delle figure GDPR fase 1	I: descrizione del processo O: individuzione figure GDPR	I: descrizione del processo O:individuazione figure GDPR		Consulenza	Consulenza
Analisi preliminare: Individuazione delle figure GDPR Fase 2	O: individuzione figure GDPR	O:individuazione figure GDPR		Consulenza	Consulenza
Analisi preliminare: Individuazione trattamenti	O: registro trattamenti, analisi preliminare	O: registro trattamenti, analisi preliminare			I: analisi preliminare O:registro trattamenti (misure di sicurezza e asset)
Macro progettazione	Consulenza	Consulenza			I: analisi preliminare O: Macroprogettazione
Progettazione di dettaglio	I: macroprogettazione O:macroprogettazione approvata	Consulenza	Consulenza		I:Macroprogettazione approvata O: progetto di dettaglio e Dossier Data Protection
Verifica GDPR del progetto di dettaglio	Consulenza	Consulenza	I: Dossier Data Protection O:Verifica misure sicurezza	I: Dossier Data Protection, verifica delle misure di sicurezza O:Emette parere su Dossier Data Protection	Consulenza
Realizzazione e messa in esercizio	I: dossier data protection verificato positivamente		O:Produce piano delle verifiche		I: progetto di dettaglio, dossier data protection,

	O:Aggiornamento registro trattamenti				O: piano di gestione

Processo gestione degli incidenti di sicurezza

Linee Guida

1 Scopo del documento

Il presente documento descrive in termini di obiettivi, attività, ruoli e responsabilità della procedura di gestione degli incidenti intesi come eventi che hanno avuto effetti negativi in termini di Data Protection o solo hanno messo in evidenza delle falle all'interno delle misure di sicurezza adottate.

15 Premessa

La presente procedura definisce le principali responsabilità ed attività relative agli obblighi di notifica verso gli Organismi di Controllo degli incidenti di Sicurezza delle Informazioni che abbiano come conseguenza la violazione di dati personali.
Ai sensi dell'art. 4 par. 12 «violazione dei dati personali» ovvero per Data Breach si definisce: "la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".

Di seguito una breve descrizione delle varie tipologie di violazione dei dati personali:

a) **Distruzione**: Indisponibilità definitiva di dati personali degli interessati con impossibilità di ripristino degli stessi entro sette giorni. La violazione può essere determinata da una eliminazione logica (es. cancellazione dei dati) oppure fisica (es. rottura dei supporti di memorizzazione) non autorizzata e relativa impossibilità di ripristinare i dati entro i sette giorni.
b) **Perdita**: Perdita del supporto fisico di memorizzazione dei dati (dischi esterni, pendrive ecc.) in termini di privazione, sottrazione, smarrimento dei dispositivi contenenti i dati degli interessati oppure dei documenti cartacei. La perdita può essere anche temporanea ma superiore a sette giorni. Può riguardare le copie o gli originali dei supporti contenenti i dati personali dei soggetti interessati.
c) **Modifica**: Modifiche improprie dei dati degli interessati non autorizzate, effettuate al di fuori dei processi operativi di trattamento dei dati svolti dagli incaricati autorizzati, oppure modifiche con finalità fraudolente eseguite dagli incaricati autorizzati all'accesso.
d) **Rivelazione**: Distribuzione non autorizzata o impropria dei dati personali degli interessati verso terze parti (persone fisiche, persone giuridiche, gruppi di soggetti, pubblico) anche non precisamente identificabili.
e) **Accesso**: Accesso non autorizzato o improprio ai dati degli interessati. Accessi ai dati (anche in sola visualizzazione, sia in caso di accessi logici ai sistemi informatici sia agli archivi cartacei) effettivamente avvenuti al di fuori dei processi operativi di trattamento dei dati previsti e autorizzati.
f) **Indisponibilità di un servizio**: quando un servizio risulta indispensabile per l'esercizio di diritti dell'interessato e per qualsivoglia motivo sia reso a lui indisponibile.

La procedura è redatta in coerenza con il Regolamento Europeo 679/2016 relativo *"alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati"* (altrimenti detto GDPR); in base alle line guida del Gruppo dei garanti (art.29) denominate "WP250 - Guidelines on Personal data breach notification under Regulation 2016/679" del 3 ottobre 2017 e sulla base delle "Indicazioni operative per la

redazione di linee guida per il processo di Data Breach" emesse da Regione Toscana il 23 maggio 2018.

Tale procedura pertanto si applica a tutti gli archivi/documenti informatici e cartacei sui cui sono conservati i dati personali degli interessati (Cittadini, dipendenti, fornitori, soggetti terzi ecc.) che la Regione e/o altri enti ad essa collegati trattano, anche attraverso il supporto di Responsabili del Trattamento.

16 Riferimenti normativi

Norme
Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
Decreto legislativo 10 agosto 2018, n. 101 che adegua il Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196) alle disposizioni del Regolamento (UE) 2016/679.
WP250 - Guidelines on Personal data breach notification under Regulation 2016/679" del 3 ottobre 2017

17 Figure organizzative e responsabilità

Nell'ambito del processo di registrazione e notifica degli incidenti entrano con diversi compiti e responsabilità, le figure elencate in tabella

Autorizzati al trattamento	Personale autorizzato dal Titolare o suo Delegato al trattamento di dati personali
DPO	Acronimo di Data Protrection Officer o Responsabile della Protezione dei Dati
Interessato	Persona fisica identificata o identificabile. Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Responsabile del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.
Security IT Manager (Data Security Officer)	Figura preposta alla supervisione ed auditing del processo di Security Management in ambito IT distinta da chi nell'organizzazione ha la responsabilità di pianificare e rendere operative le misure di sicurezza secondo il principio Separation of Duty richiamato nello stesso GDPR. *(la*

	separazione dei compiti, è un concetto chiave per l controlli interni e viene raggiunto suddividendo un processo di sicurezza fra più persone, tipicamente, fra chi mette in atto e chi controlla)
Titolare del trattamento o suo Delegato	la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.
Responsabile Sicurezza delle Infrastrutture	ła figura che, nell'ambito di propria competenza, ha la responsabilità dei livelli di sicurezza IT attraverso la pianificazione, messa in opera e gestione di adeguate misure, Mantiene il catalogo degli asset infrastrutturali, delle minacce e delle misure adottate.
Responsabile Sistema Informativo	La figura responsabile, nell'ambito della sua area di competenza, dell'analisi, dello sviluppo e della gestione delle applicazioni IT costituenti i diversi sistemi informativi. Nei suoi compiti l'adozione di misure di sicurezza idonee contro minacce di tipo applicativo, a tale scopo mantiene aggiornato il catalogo degli asset (applicazioni), delle minacce e delle misure adottate.

Le figure organizzative indicate nel paragrafo precedente sono coinvolte nel processo di registrazione e notifica degli incidenti così come delineato nella seguente tabella.

Ruolo / Struttura	Responsabilità principali relative alla Procedura
Autorizzati al trattamento	Comunicare con qualsiasi strumento (email, telefono, specifiche applicazioni e/o APP per la segnalazione degli incidenti, personalmente) ai Delegati del Titolare (per i trattamenti di loro diretta responsabilità) ogni incidente o sospetto di incidente di sicurezza che possa coinvolgere, anche solo potenzialmente, dati personali. comunicazione da parte degli interessati al DPO attraverso i contatti pubblicati.
Titolare o Delegato del Titolare (Dirigenti / Direttori)	Ricevere e gestire la segnalazione del potenziale incidente; Collaborare con il Security Manager e un eventuale gruppo di specialisti di sicurezza, da lui individuato, nella ricostruzione degli accadimenti dell'incidente di sicurezza; Supportare il Security Manager nelle relazioni con eventuali Responsabili di trattamenti esterni; Provvedere – se necessario – a notificare l'incidente all'Autorità Garante per la protezione dei dati personali, di concerto con Il DPO Procedere – se necessario – a comunicare l'incidente agli Interessati, di concerto con il DPO Formare periodicamente il proprio personale per l'individuazione e segnalazione degli incidenti sui dati personali.
Security Manager o (DSO) Data Security Officer	Predispone la realizzazione e gestione del registro elettronico degli incidenti di Data Protection. Coordina il gruppo di specialisti della sicurezza (interni o esterni) al fine di effettuare tutte le indagini e analisi sull'accaduto; Gestisce in collaborazione con il DPO le comunicazioni di incidenti; Richiede al responsabile della sicurezza delle infrastrutture e al responsabile sistemi informativi o a figure equivalenti, dettagliata documentazione sull'evento occorso, sulle misure di contenimento e rimedio messe in campo o pianificate e i relativi tempi.

Ruolo / Struttura	Responsabilità principali relative alla Procedura
	Si interfaccia agli eventuali Responsabili (se presenti) per ricevere ulteriori informazioni sull'accaduto e/o per definire le eventuali responsabilità di fornitori esterni; Predispone le comunicazioni interne (automatiche o manuali) al DPO e al Titolare sull'accaduto e sugli approfondimenti in corso; Supervisiona il lavoro del gruppo degli specialisti della sicurezza addetti al contrasto dell'incidente; Aggiorna il registro degli incidenti elettronico in base all'esito degli eventi successivi all'incidente (azioni di contrasto e indagini di approfondimento); Supporta se richiesto il titolare e il DPO nelle decisioni di comunicazione degli incidenti al Garante; Supporta se richiesto il titolare e il DPO nelle decisioni di comunicazione degli incidenti agli interessati.
Responsabili del trattamento	Rilevano e registrano gli incidenti in ambito Data Protection che si verificano sui dati personali presenti in archivi o Sistemi Informativi da essi utilizzati, notificandoli contestualmente sia al Security Manager sia ai Delegati del Titolare per i trattamenti di loro diretta responsabilità; Valutano l'impatto dell'incidente di Sicurezza sugli interessati per i servizi prestati; Supportano il Security Manager e il gruppo di specialisti di sicurezza nella ricostruzione degli accadimenti dell'incidente di sicurezza.
DPO	Supervisiona le attività legate al processo complessivo di notifica degli incidenti di sicurezza delle informazioni in ambito Data Protection. Coadiuva e supporta il titolare nelle decisioni di comunicazione degli incidenti al Garante; Coadiuva e supporta il titolare nelle decisioni di comunicazione degli incidenti agli interessati; Acquisisce e archivia per i processi di Analisi dei rischi (compreso le DPIA) e di Accountability i dossier prodotti dal registro elettronico sugli incidenti di sicurezza avvenuti; Effettua verifiche periodiche con audit sulla efficacia del processo di notifica degli incidenti di sicurezza delle informazioni in ambito Data Protection.
Responsabile della Sicurezza delle Infrastrutture	Informa obbligatoriamente il Security Manager (DSO) in merito alla rilevazione di incidenti; collabora attivamente nella fase di gestione degli incidenti al fine sia della loro risoluzione sia degli adempimenti richiesti dal GDPR ed è responsabile dei tempi di notifica; comunica periodicamente al Security Manager (DSO) le misure di sicurezza adottate; collabora nelle azioni di verifica, delle misure di sicurezza, messe in atto dal Security Manager; si conforma nei tempi e nei modi indicati dal Security Manager e confermati dal DPO, per il miglioramento delle misure di sicurezza.
Responsabile Sistemi informativi	Informa obbligatoriamente il Security Manager in merito alla rilevazione di incidenti; collabora attivamente nella fase di gestione degli incidenti al fine sia della loro risoluzione sia degli adempimenti richiesti dal GDPR ed è responsabile dei tempi di notifica; comunica periodicamente al Security Manager misure di sicurezza adottate; collabora nelle azioni di verifica, delle misure di sicurezza, messe in atto dal Security Manager; si conforma nei tempi e nei modi indicati dal Security Manager e confermati dal DPO, per il miglioramento delle misure di sicurezza.
Responsabile dell'Archivio / Responsabile del	Informa obbligatoriamente il Security Manager in merito alla rilevazione di incidenti su dati conservati su supporti cartacei;

Ruolo / Struttura	Responsabilità principali relative alla Procedura
patrimonio	collabora attivamente nella fase di gestione degli incidenti al fine sia della loro risoluzione sia degli adempimenti richiesti dal GDPR ed è responsabile dei tempi di notifica; comunica periodicamente al DPO le misure di sicurezza adottate;

18 Modalità Operative

Per ogni dettaglio e approfondimento relativamente al quadro normativo in cui si colloca il processo di Data Breach, per gli adempimenti prescritti dalla normativa; i soggetti ed i ruoli; la tipologia di violazioni ed eventi e la panoramica sui processi operativi di rilevazione e segnalazione delle violazioni dei dati personali, si deve fare riferimento al documento di "Indicazioni operative per la redazione di linee guida per il processo di Data Breach" approvate da Regione Toscana con DGR 585 del 23 maggio 2018, che costituisce parte integrante del presente documento.

19 Attivazione della procedura di notifica degli incidenti

La procedura è attivata da chiunque venga a conoscenza, anche casualmente, di incidenti o potenziali incidenti di sicurezza nell'ambito della sicurezza delle informazioni, che abbiano come conseguenza la violazione di dati personali.
Il soggetto segnalatore può essere, a titolo di esempio, il responsabile della sicurezza delle infrastrutture o un suo collaboratore; il responsabile dei sistemi informativi o un suo collaboratore; il responsabile dell'archivio o un suo dipendente, un dipendente dell'ente (incaricato o meno di operare sui trattamenti), un collaboratore esterno; un dipendente di un fornitore; un Responsabile di trattamento; un operatore del call center; un addetto all'ufficio Relazioni con il pubblico, un interessato, ecc.
Il soggetto segnalatore, attraverso un qualsiasi canale di comunicazione messo a disposizione per la segnalazione di incidenti (email, telefono, specifiche applicazioni e/o APP per la segnalazione degli incidenti, personalmente) contatta il DPO e/o il Security Manager (DSO).
Il DSO (Security IT Manager) è il soggetto che prende in carico la segnalazione dell'incidente e provvede alle seguenti azioni:

a. Apre la registrazione dell'incidente (data, ora, segnalatore, descrizione della segnalazione);
b. individua il Responsabile della sicurezza delle infrastrutture o il Responsabile del sistema informativo interessato;
c. nel caso di incidenti che coinvolgono informazioni custodite in archivi cartacei coinvolge il responsabile dell'Archivio;
d. ottiene le maggiori informazioni possibili in merito all'incidente al fine di individuare in collaborazione con l'ufficio DPO, i trattamenti coinvolti e i relativi titolari delegati, la natura dei dati coinvolti nell'incidente, le categorie e la numerosità degli interessati;
e. Informa il titolare delegato dei trattamenti coinvolti e aggiorna il registro degli incidenti.

Il Titolare o sui Delegati provvedono ad effettuare formazione periodica sul proprio personale a riguardo della individuazione e segnalazione degli incidenti di sicurezza sui dati personali.

Nel caso in cui si verifichi un evento di violazione dei dati personali trattati nell'erogazione del servizio da parte di un Responsabile (fornitore esterno), lo stesso effettua una prima analisi dell'accaduto, invia la segnalazione al Security Manager (DSO) del Titolare o suo Delegato per la quale eroga il servizio, senza ingiustificato ritardo (immediatamente) da quando è venuto a conoscenza della violazione. La segnalazione deve contenere tutti gli elementi utili alla comprensione/identificazione dell'evento (trattamenti coinvolti, tipologia di dati, categorie e numerosità degli interessati, modalità dei trattamenti, attori coinvolti, ..).

Il fornitore garantisce inoltre assistenza al DSO, al DPO, al Titolare o suo Delegato del servizio, fornendo eventuali informazioni aggiuntive per la corretta valutazione e gestione dell'evento.
Il Titolare o suo Delegato ha la responsabilità, nell'ambito degli accordi e contratti fra Titolare e Responsabile, di normare gli obblighi e modalità di segnalazione degli incidenti di sicurezza verso il sistema organizzativo dell'ente. In sostanza deve essere individuato il punto di contatto e fornita l'istruzione per seguire la presente linea guida.

20 Gestione ciclo di vita dell'incidente

Il Titolare o suo Delegato una volta ricevuta la segnalazione, provvede ad aggiornare per le parti di propria competenza, il registro degli incidenti in riferimento alle valutazioni in merito ai rischi o danni che l'incidente può causare agli interessati.
Il DSO provvede ad aggiornare i dati relativi all'incidente in relazione:

1. alla minaccia rilevata;
2. alle modalità di accadimento;
3. alle motivazioni di non presenza di adeguate misure di contrasto;
4. alle misure adottate di contenimento;
5. alle misure e ai tempi programmati per l'attuazione di azioni di rimedio.

L'applicativo per la gestione del Registro degli incidenti, consente di inserire tutte le informazioni utili alla valutazione degli accadimenti e loro severità. Il registro consente inoltre di gestire tutto il processo di incident management, compresa la registrazione dei tempi, fino alla eventuale comunicazione al garante e agli interessati archiviando anche i contenuti delle comunicazioni stesse.
Una volta aperto l'incidente, da parte del DSO, il Registro provvede ad inviare in automatico una prima comunicazione sia al Titolare o suo Delegato sia al DPO della presenza di un nuovo evento di sicurezza all'interno dello stesso Registro.
L'incidente viene chiuso formalmente dal Titolare o suo delegato con il supporto del DSO, che accerterà e verificherà che siano state effettuate le comunicazioni del caso e pianificati gli interventi di risoluzione.
La documentazione relativa all'incidente confluisce all'interno del "Dossier Data Protection" riferito al processo produttivo nell'ambito del quale è avvenuto.

21 Indagini e approfondimenti tecnici

Una volta ricevuta la segnalazione di un nuovo evento, il Security Manager valuta la completezza delle informazioni e, se necessario, dispone degli approfondimenti tecnici ed organizzativi sugli accadimenti oggetto dell'indagine.
Qualora sia necessario, il Security Manager può creare un pool di specialisti al fine di farsi supportare nelle attività di indagine ed approfondimento.
Qualora l'incidente di sicurezza abbia coinvolto archivi cartacei le indagini e gli approfondimenti sono delegati al responsabile dell'Archivio e/o del Patrimonio.
Scopo dell'attività di indagine del Security Manager è raccogliere informazioni a riguardo di:

1) natura della violazione dei dati personali;
2) categorie di soggetti interessati;
3) il numero approssimativo di interessati;

4) il numero approssimativo di registrazioni;
5) dati personali coinvolti nella violazione;
6) tipologia di violazione delle informazioni;
7) tassonomia dell'evento;
8) dispositivi coinvolti nella violazione;
9) capacità di identificare le persone coinvolte nella violazione;
10) probabili conseguenze della violazione dei dati personali;
11) classificazione della severità dell'evento;
12) eventuali vulnerabilità individuate;
13) eventuali misure preventive adottate.

22 Valutazione della probabilità di rischio per i diritti e le libertà degli Interessati

Il Titolare o suo Delegato, avvalendosi anche del supporto del Security Manager e del DPO, deve valutare se l'incidente può comportare un rischio per i diritti e le libertà delle persone fisiche, ovvero se può cagionare un danno fisico, materiale o immateriale alle persone fisiche, tale da provocare una o più tra le seguenti conseguenze:

a. discriminazioni;
b. furto o usurpazione di identità;
c. perdite finanziarie;
d. pregiudizio alla reputazione;
e. perdita di riservatezza dei dati personali protetti da segreto professionale;
f. decifratura non autorizzata della pseudonimizzazione;
g. qualsiasi altro danno economico o sociale significativo.

Se, in base alla valutazione di tali parametri, il Titolare o suo Delegato ritiene che l'incidente rappresenti un **rischio PROBABILE** o **ELEVATO** per i diritti e le libertà delle persone fisiche, procede alla notifica al Garante per la protezione dei dati personali, come indicato nel paragrafo 5.6.

Diversamente non viene emanata alcuna notifica.

Il Titolare o suo Delegato aggiorna il Registro degli incidenti con le seguenti informazioni:

1. Capacità di identificare le persone coinvolte nella violazione;
2. probabili conseguenze della violazione dei dati personali;
3. classificazione della severità dell'evento;
4. livello di rischio finale;
5. necessità di comunicazione dell'evento al garante.

23 Notifica dell'incidente al Garante per la protezione dei dati personali

Nel caso in cui si sia valutato un rischio PROBABILE o ELEVATO nella valutazione per i diritti e le libertà degli Interessati, il Titolare del trattamento o suo Delegato, avvalendosi anche del

supporto del DPO e del Security Manager, deve provvedere alla comunicazione al Garante secondo le seguenti modalità e tempi in base al dato coinvolto nell'incidente di sicurezza:

Tabella 1

Tipologia dati coinvolti	Provvedimento di riferimento per la comunicazione	Entro	Modalità di comunicazione
Descrizione dei dati	Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016	72 ore	Modulo sito garante Privacy

Nel caso in cui la valutazione di rischio per i diritti e le libertà degli interessati effettuata al paragrafo 5.5 abbia evidenziato un **rischio ELEVATO** occorre in particolare raccogliere e documentare all'interno del Registro degli incidenti le informazioni sulle "Misure preventive" e "Misure correttive" per verificare se:

a. **prima dell'incidente** ai dati personali oggetto della violazione erano state applicate misure di protezione adeguate (in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura) [Art. 34, comma 3° del Regolamento 2016/679];
b. a seguito dell'incidente sono state adottate misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati [Art. 34, comma 3b del Regolamento 2016/679].

c. Se nessuna delle due condizioni precedenti è soddisfatta, occorre procedere anche alla comunicazione dell'incidente agli Interessati, come previsto al paragrafo 5.7
d. Diversamente è sufficiente la notifica al Garante.

Il modulo compilato, deve essere inviato al Garante per la protezione dei dati personali **entro le 72 ore dal momento in cui si è venuti a conoscenza dell'incidente**, attraverso i canali indicati nel modulo stesso.

Nel caso in cui non sia possibile inoltrare la notifica al Garante con tutte le informazioni richieste entro i tempi prescritti, è necessario comunque inviare al garante la notifica della violazione, con le prime indicazioni raccolte con l'indicazione delle ragioni del ritardo. Le ulteriori informazioni di dettaglio sull'incidente saranno comunicate successivamente senza ingiustificato ritardo. Le ragioni del ritardo vanno inoltre riportate nella apposita sezione all'interno del registro degli incidenti.

24 Comunicazione dell'incidente agli interessati

Il Titolare del trattamento o suo Delegato, avvalendosi anche del supporto del Security Manager e del DPO, deve valutare la necessità di procedere anche alla comunicazione dell'incidente a tutti gli Interessati, ossia a tutte le persone fisiche i cui dati personali possono essere stati violati.

Una violazione di dati personali, ovvero *"una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati"* deve essere comunicata a tutti gli Interessati quando occorrono le seguenti condizioni:

a. Prima dell'incidente ai dati personali oggetto della violazione non erano state applicate misure tecniche e organizzative di protezione adeguate (es. cifratura, anonimizzazione, pseudonimizzazione), atte cioè a limitare efficacemente il rischio di furto d'identità o altre forme di abuso;

e inoltre:

b. A valle dell'incidente non è stato possibile mettere in atto misure tecniche e organizzative in grado di porre rimedio alla violazione dei dati personali e/o di attenuarne i possibili effetti negativi, scongiurando così il sopraggiungere di un **rischio ELEVATO** per i diritti e le libertà degli Interessati.

In questo caso il Titolare del trattamento o suo Delegato deve provvedere a comunicare l'incidente agli Interessati **senza ingiustificato ritardo**, attraverso una apposita comunicazione che descriva con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contenga almeno le seguenti informazioni:

a. Il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui l'Interessato possa ottenere più informazioni;
b. una descrizione della violazione dei dati personali, che includa ove possibile informazioni sul numero e le categorie degli interessati;
c. una descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Il contenuto sintetico della comunicazione agli interessati va riportato all'interno della sezione specifica nel Modulo di Notifica e all'interno del Registro degli incidenti.

Qualora il DPO ritenga che l'invio di questa comunicazione a tutti gli Interessati richiederebbe sforzi sproporzionati (ad es. a causa della elevata numerosità degli Interessati da contattare), può decidere in alternativa di optare per una comunicazione pubblica.

25 Comunicazione pubblica

Il Titolare del trattamento o suo Delegato, in accordo con le Funzioni dell'Ente preposte alla gestione dei rapporti con il pubblico e con i media, deve provvedere ad effettuare **senza ingiustificato ritardo** una comunicazione pubblica relativa all'incidente relativo alla violazione di dati personali.

Tale comunicazione pubblica (o misura simile) deve essere in grado di informare gli Interessati relativamente alla violazione dei loro dati personali con chiarezza ed efficacia analoghe alla comunicazione diretta (v. paragrafo 5.7)

Utilizzando i canali istituzionali per le comunicazioni con il pubblico (sito WEB, comunicazioni agli sportelli), attraverso i media (stampa, tv, radio) o altre forme di contatto in grado di garantire

che tutti gli interessati possano essere raggiunti, dovrà essere diramato un comunicato che descriva con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contenga almeno le seguenti informazioni:

a. Il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui l'Interessato possa ottenere più informazioni;
b. una descrizione della violazione dei dati personali, che includa ove possibile informazioni sul numero e le categorie degli interessati e delle probabili conseguenze della violazione dei dati personali;
c. una descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Il contenuto sintetico della comunicazione pubblica va riportato all'interno della sezione specifica nel Modulo di Notifica e all'interno del Registro degli incidenti.

26 Comunicazione all'autorità giudiziaria

Qualora l'incidente si configuri come atto doloso Il titolare o suo delegato in collaborazione con il Security Manager e il DPO, procede alla comunicazione dell'evento all'autorità giudiziaria.

27 Registro incidenti

L'art 33 paragrafo 5 del GDPR prevede "Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo".
L'Applicativo per la gestione del Registro degli incidenti in ambito Data Protection deve far parte obbligatoriamente della policy di sicurezza dell'ente e deve essere realizzato e gestito tenendo conto di quanto richiesto dall'art. 33, utilizzato come strumento di raccolta ed identificazione di un possibile Data Breach e per la valutazione del livello di rischio dello stesso.
Il registro oltre a tracciare tutte le informazioni richieste dalla normativa vigente e necessarie alla corretta gestione del processo di Incident Management, è in grado di fornire tutta la documentazione raccolta, su richiesta, al Garante in caso di accertamenti.
L'applicativo per la gestione del Registro degli incidenti in ambito Data Protection è in grado inoltre di produrre un Dossier con tutta la documentazione e le informazioni raccolte per ogni singolo evento da trasferire nel sistema di archiviazione documentale.
In sintesi, il registro rappresenta lo strumento del titolare, affidato alla gestione del Security manager, attraverso il quale fa fronte al principio di accountability relativamente agli incidenti occorsi, alle loro motivazioni, ai rimedi intrapresi, ai rischi o danni causati e alle comunicazioni effettuate.

28 Modalità di controllo

L'applicazione della procedura è monitorata mediante audit interni periodici condotti dal Security Manager e dal DPO.

29 Strumenti Informativi coinvolti

a) ***Registro degli incidenti in ambito Data Protection***
b) ***Dossier Data Protection del processo o processi coinvolti nell'incidente***
c) ***Catalogo degli asset e relative misure di sicurezza***
d) ***Fascicolo dell'interessato***

Processo di Accountability
Linee Guida

1 Scopo del Documento

Il presente documento costituisce linea guida per l'attuazione del processo tecnico ed organizzativo che l'ente, è tenuto a porre in essere al fine di ottemperare al principio dell'accountability. Quest'ultimo è richiamato nell'art. 24 del Reg. UE n. 679/2016 (di seguito indicato con l'acronimo GDPR) e definito come l' *"..essere in grado di dimostrare che il trattamento è effettuato conformemente al presente regolamento.."* e ne costituisce uno dei principi cardine. Occorre, a tal proposito, sottolineare che anche grazie all'importanza attribuita al principio dell'accountability nel GDPR, è mutato l'approccio proposto alla materia della protezione dei dati, rispetto a quello che caratterizzava il D.Lgs. n. 196/2003 (Codice della Privacy), attualmente modificato dal D.Lgs. n. 101/2018 di armonizzazione della normativa nazionale al GDPR. L'accontability si sostanzia essenzialmente nei seguenti aspetti:

a. Accountability organizzativa e cioè come è stata modificata l'organizzazione per l'attuazione del GDPR,
b. Accontability di processo e cioè come si è dato luogo in termini di obiettivi, attività, ruoli e responsabilità alla messa in atto dei principi e delle indicazioni del GDPR
c. Accountability Tecnica/Organizzativa e cioè quali sono state le misure di sicurezza adeguate, messe in atto

La presente "Linea Guida per l'accountability" ha lo scopo di tracciare un elenco di **strumenti e di attività** che dovranno essere compiute e costantemente monitorate, al fine di rendere evidente e concreta la conformità al principio dell'accountability.

30 Premessa

Il principio di accountability, può sintetizzarsi nella capacità di "rendere conto"/comprovare le azioni effettuate, e tratteggia una responsabilizzazione dei soggetti coinvolti in materia di protezione dei dati personali: questi ultimi, infatti, secondo quanto previsto dal dettato normativo, non dovranno più adottare un approccio di formale adempimento alle norme, ma un approccio cosiddetto sostanziale, ponendo al centro la tutela dei dati personali.
In tal senso il principio di accountability deve essere letto sotto un duplice profilo: esso non solo è il principio che ispira l'adeguamento/l'adempimento degli enti alla normativa europea, ma è anche il punto di partenza per **dimostrare** la compliance (il rispetto, l'aderenza) dell'ente/organizzazione alla norma europea.
Il principio di accountability è quindi inevitabilmente connesso – in quanto ne costituisce il presupposto logico/sistematico – a ciascun processo di trattamento di dati personali, dettandone le regole di evidenza documentale e procedurale, con peculiare riferimento al processo di istituzione, conservazione ed aggiornamento del **registro dei trattamenti**, che grava in capo ai Titolari ed ai Responsabili del trattamento e che consente di avere una chiara panoramica dei trattamenti di dati personali effettuati all'interno dell'organizzazione, nonché al processo di istituzione e conservazione del **registro degli incidenti (e alla relativa procedura organizzativa)**, ove si mantiene traccia degli eventi di violazione dei dati personali (***Data Breach***) e delle decisioni assunte in merito ad essi, sia di carattere tecnologico, sia amministrativo (comunicazioni all'autorità di controllo-Garante Privacy, agli interessati, all'autorità giudiziaria).
Il suddetto principio è, altresì, correlato alla **Valutazione di impatto** (***DPIA***), eventualmente effettuata per i trattamenti caratterizzati da un elevato rischio di pregiudizio ai diritti e alle libertà degli interessati.
In conclusione, come già emerso dalla disamina condotta, ciò che muta è l'atteggiamento della normativa rispetto alla tematica della protezione dei dati personali, che impone una riflessione

preventiva rispetto alla materia *de qua*, per adattare l'organizzazione in base alle opportunità che si intendono cogliere, lasciando non solo ampi spazi di autonomia ai soggetti Titolari/Responsabili, ma anche abbandonando quell'approccio di mero adempimento che aveva caratterizzato la vigenza della precedente normativa privacy. In sintesi, non è sufficiente avere "le carte a posto".
Il principio dell'accountability si affianca ad altro principio cardine del Regolamento Europeo, quello della data protection by design, che necessita dell'attuazione di idonee procedure per essere garantito e per consentire anche il raggiungimento del principio dell'accountability.

31 Oggetto del documento

L'accountability è l'approccio pratico al trattamento dei dati personali: mira allo sviluppo di strumenti/supporti che possano essere utilizzati per documentare le proprie attività sui dati personali e renderne conto alle autorità di controllo, agli interessati (capo III del GDPR) ed all'autorità giudiziaria.
L'accountability costituisce un principio cardine anche per i trattamenti di dati che la Regione Toscana, in veste di titolare, affida a Responsabili del trattamento ex art. 28 GDPR, in quanto gli standard del trattamento (in termini tecnici ed organizzativi) devono essere garantiti dall'intera filiera di soggetti coinvolti (titolare/i, responsabile/i e subresponsabile/i), ai quali il titolare si affida.

32 Strumenti per il processo di Accountability

Esistono tre livelli di compliance al GDPR che forniscono le basi per l'Accountability:

a. ***la compliance organizzativa,*** che descrive come l'organizzazione si è modificata al fine di rispondere adeguatamente alle direttive del GDPR;
b. ***la compliance di processo,*** che descrive come si siano modificati o aggiunti processi produttivi e procedimenti amministrativi, al fine di rispettare le direttive del GDPR; al suo interno si colloca la ***compliance tecnica,*** che descrive le misure tecniche di cui la titolare si è munita per tutelare idoneamente i dati personali affidati, in base alle caratteristiche intrinseche del trattamento (natura, tipologia di dati, etc.) ed ai livelli di rischio connessi.

33 Compliance organizzativa

La compliance organizzativa è dimostrabile grazie ad un insieme di atti, provvedimenti e documenti che descrivono gli interventi organizzativi strutturali e gli strumenti messi in atto dall'organizzazione.

34 Documenti e strumenti

Documenti:

1. linee guida per l'accountability;
2. atto di nomina del DPO/RPD;
3. linee guida per l'organizzazione e loro attuazione;
4. linee guida per la data protection by design;
5. linee guida per il registro dei trattamenti;
6. linee guida per la gestione degli incidenti e procedure di data breach;
7. linee guida per la tutela dei diritti degli interessati;

8. report periodico circa l'attività di informazione e formazione del personale (attuata sia con lezioni frontali in aula sia tramite FAD);
9. report periodico su registro dei trattamenti;
10. linee guida per la garanzia dei diritti degli interessati;
11. disciplinare sulla posta elettronica;
12. disciplinare su uso dei social;
13. disciplinare per protocollo ed archivi cartacei;
14. disciplinare per la conservazione a norma;
15. misure di sicurezza relative alle stazioni di lavoro e alla rete interna;
16. misure di sicurezza richieste a fornitori sia nel ciclo di vita dello sviluppo di applicazioni, sia nella loro gestione e nella gestione dei dati;
17. piano di lavoro relativo al continuo processo di adeguamento e miglioramento del rispetto al GDPR;

Strumenti:

a. repository documentale che archivi e tenga traccia delle versioni dei documenti;
b. applicazione del registro dei trattamenti che produca con periodicità mensile il registro dei trattamenti in forma scritta e che consenta in qualsiasi momento l'accesso ai trattamenti con profili autorizzativi per funzionalità ispettive e di controllo.

35 Compliance di processo

La compliance di processo si sostanzia nel mettere in atto le misure delineate dalle linee guida e dai processi di monitoraggio e controllo.
I principali processi derivanti dall'adozione del GDPR, per il dettaglio dei quali si rimanda alle specifiche linee guida sono:

1. Data Protection by Design;
2. Gestione degli incidenti, monitoraggio e verifica;
3. Garanzia dei diritti degli interessati;
4. Accountability di cui il presente documento costituisce esso stesso la linea guida.

Per ciascuno dei su indicati processi definiremo i principali documenti e strumenti idonei a dimostrare la loro attuazione e consentire la verifica sull'efficacia delle misure poste in essere.

35.1 Data Protection by Design

Il processo di Data Protection by Design contiene al suo interno il sottoprocesso di gestione dei trattamenti di cui è parte integrante il registro dei trattamenti e il sottoprocesso di valutazione dell'impatto per i temi di Data Protection (DPIA).

35.1.1 Documenti e strumenti

Documenti:

Tra i documenti chiave, che a posteriori possono illustrare il processo che ha condotto alle scelte tecniche e organizzative relative all'avvio di uno o più trattamenti che coinvolgono dati

personali, vi è il ***Dossier Data Protection.*** Esso contiene gli output del processo di Data Protection by Design nelle varie fasi, dall'emersione del "bisogno" alla messa in atto del processo organizzativo e tecnologico idoneo a fornire un'adeguata risposta al "bisogno" sorto, comprensivo degli atti che ne caratterizzano la gestione successiva:

1. atto che istituisce un nuovo processo o ne modifica uno esistente (legge, regolamento delibera, decreto) e descrizione del processo;
2. individuazione del modello organizzativo e descrizione del processo in termini di mappatura dei ruoli organizzativi e delle figure previste dal GDPR (Titolari, Responsabili ecc.) e relative interrelazioni (titolare con titolare, titolare con responsabile ed eventualmente sub responsabile, rapporti di contitolarità);
3. contratti che regolano le responsabilità dei diversi attori coinvolti nel processo;
4. eventuale DPIA realizzata (output software DPIA);
5. individuazione dei trattamenti e loro registrazione nel registro dei trattamenti;
6. soluzioni tecniche ed architetturali messe in atto e relative misure di sicurezza;
7. pareri, indicazioni o prescrizioni del DPO;
8. incidenti occorsi e loro risoluzione.

Strumenti:

Al fine di rendere attuabile la formazione e la gestione del predetto ***Dossier*** occorre:

1. collegare (come indicato nelle linee guida organizzative e del processo di data Protection by design), le procedure amministrative degli atti con il processo di data protection by design;
2. disporre di una repository dei dossier;
3. disporre di una procedura per la gestione dei pareri e delle prescrizioni del DPO dalla richiesta alla formalizzazione definitiva.

35.2 Gestione Incidenti, monitoraggio e verifica

Il processo di gestione degli incidenti, nel suo complesso, si configura come un processo di auditing continuativo da parte del Security IT Manager sull'effettiva messa in pratica delle misure di sicurezza e sulla loro efficacia. Per far ciò vengono programmate specifiche attività al verificarsi di incidenti di sicurezza o di eventi che comunque hanno un impatto su temi relativi al GDPR. Per i contenuti e le modalità di gestione del registro degli incidenti si rimanda alle relative linee guida.

35.2.1 Documenti e strumenti

Documenti:

1. produzione in forma scritta (PDF firmato) del registro degli incidenti con indicazione del processo e quindi del Dossier Data Protection di riferimento e delle misure poste in essere come remediation plan;
2. produzione degli esiti di interventi periodici di monitoraggio e controllo circa la messa in atto di misure di sicurezza adeguate ed in relazione alla loro efficacia.

Strumenti:

1. sistema di rilevazione e gestione degli incidenti collegato alla gestione dei dossier data protection ed al registro dei trattamenti;
2. sistema di monitoraggio e verifica delle misure di sicurezza adottate e registrazione dei punti di debolezza rilevati e delle relative proposte/prescrizioni di adeguamento.

35.3 Garanzia dei diritti dell'interessato

Il processo di "tutela dei diritti dell'interessato" ha l'obiettivo di garantire agli "interessati" un'adeguata risposta alle richieste derivanti dall'esercizio dei loro diritti, come indicati al capo III del GDPR.
La suddetta richiesta sia che si configuri come "segnalazione", sia che assuma la forma di una richiesta "vera e propria" avente ad oggetto quanto previsto al Capo III con particolare riferimento a:

1. art. 12-14 (informativa);
2. art. 15 (accesso) e art. 19 (notifica);
3. art. 16 (rettifica);
4. art. 17 (oblio);
5. art. 18 (limitazioni al trattamento);
6. art. 20 (portabilità);
7. art. 21 (opposizione);
8. art. 23 (limitazioni);

La richiesta viene inviata dall'interessato al DPO o al Titolare, che se ne fa carico e risponde nei tempi prefissati dallo stesso GDPR.
Ogni richiesta viene registrata, così come la risposta fornita ad ogni richiesta presentata.
In adempimento a quanto previsto all'art. 19 del GDPR, si mantiene traccia delle richieste di accesso e delle richieste di portabilità dei propri dati effettuate dagli interessati, così da essere in grado di informarli di eventuali successive modifiche derivanti da attuazione degli articoli 16, 17, 18, 23 del GDPR.

35.3.1 Documenti e strumenti

Documenti:

1. segnalazione/richiesta dell'interessato;
2. risposta da parte del Titolare/DPO alla richiesta presentata.

Strumenti:

1. procedura web per l'accettazione di segnalazioni/richieste;
2. gestione dell'archivio delle richieste e delle risposte formulate;
3. fascicolo dell'interessato, inteso come un master index avente come chiave l'identificativo (codice fiscale) dell'interessato, che descrive su quali banche dati sono memorizzate le informazioni dell'interessato, le categorie di queste informazioni, i trattamenti che prevedono l'uso di dette banche dati.

4. sistemi per l'estrazione di dati e trasferimento degli stessi all'interessato che ne faccia richiesta.

35.4 Piano delle verifiche periodiche (monitoraggio)

La responsabilità delle attività di verifica connesse all'attuazione del principio di accountability è in capo all'ufficio del DPO, che si avvale delle strutture dell'ente ed in particolare del responsabile dei sistemi informativi, del responsabile delle Infrastrutture Information Technology, del Security IT manager e del responsabile del sistema di documentazione ed archivi per lo svolgimento delle stesse.

Il DPO, nell'ambito del presente documento, definisce le metodologie delle verifiche periodiche rendendole note al Titolare attraverso l'Assessore competente, alla Direzione Generale, all'Avvocato Generale, ai Direttori e ai Dirigenti in quanto delegati dal Titolare.

Il DPO ogni anno dovrà emettere un piano delle verifiche periodiche a cui le strutture nell'ambito delle loro competenze dovranno attenersi. Il piano, per esigenze operative o strategiche, potrà subire variazioni in corso d'opera che saranno anch'esse preventivamente comunicate.

Le verifiche dovranno essere eseguite con la doppia finalità di individuare eventuali carenze di conformità e contestualmente ottenere una documentazione che comprovi, per quanto possibile, l'ottemperanza al principio di accountability.

I risultati ottenuti saranno oggetto di valutazione nell'ambito della relazione che il DPO formulerà al Titolare e suoi delegati, oltre che ai responsabili delle strutture; questi ultimi, seguendo le indicazioni delineate in relazione, dovranno promuovere azioni tese a migliorare il livello di sicurezza tecnica e organizzativa ed a colmare eventuali carenze riscontrate in merito alla protezione di dati personali.
Per tale attività che ricade in quanto previsto all'art. 39 del GDPR, l'amministrazione, nel suo ruolo di Titolare, dovrà mettere a disposizione del DPO risorse idonee a svolgere il compito (art. 38, comma 2, del GDPR).

35.4.1 Il piano delle verifiche sui trattamenti

L'ufficio del DPO, avvalendosi delle risorse messe a disposizione dall'amministrazione, predispone un piano annuale e lo attua previa comunicazione all'amministrazione stessa in relazione ai punti descritti nei paragrafi che seguono.

35.4.2 Completezza rispetto alla realtà, dei trattamenti in essere nell'organizzazione

Viene svolta:

1. un'indagine campionaria dei trattamenti delle Direzioni e si procede, tramite interviste, alla verifica della loro reale sussistenza ed all'aggiornamento fra quanto presente nel registro e quanto rilevato in concreto;

2. una rilevazione attuata confrontando trattamenti presenti nel registro ed applicazioni IT in esercizio. Se attivo catalogo delle applicazioni IT si procederà su tutto l'universo, altrimenti si opererà su un campione di applicazioni.

35.4.3 Completezza delle informazioni nel registro

Al fine della verifica della completezza ed aggiornamento delle informazioni presenti sul registro si procederà:

1. alla verifica della rispondenza fra dirigenti cessati e dirigenti ancora presenti eventualmente nel registro;
2. alla verifica della corretta individuazione ed aggiornamento delle strutture verificando se a cambiamenti organizzativi (modifiche di strutture) siano seguiti corrispondenti cambiamenti nel registro dei trattamenti;
3. verifica che gli autorizzati siano personale in servizio e siano collocati all'interno delle strutture competenti a quel trattamento;
4. verifica a campione sulle applicazioni che gli accessi autorizzati lo siano a dipendenti o persone classificate nel registro come "autorizzati";
5. verifica nel registro delle misure di sicurezza presenti.

35.4.4 Corretta individuazione delle norme di riferimento

Verifica a campione circa la presenza nel registro, per ogni trattamento, delle norme che ne determino la loro liceità e loro corretta individuazione.

35.4.5 Corretta individuazione delle figure DP in gioco

Verifica a campione sulla corretta individuazione, all'interno del registro dei trattamenti, dei ruoli Data Protection previsti dal GDPR (Titolari, Responsabili, Sub Responsabili, Contitolari) e sull'indicazione nello stesso dei riferimenti a contratti o convenzioni che regolano i rapporti tra le figure GDPR sopra richiamate.

35.4.6 Corretta compilazione di contratti/convenzioni

Verifica a campione sulla corretta redazione dei contratti o convenzioni che regolano i rapporti fra le figure GDPR, presenti nel registro dei trattamenti.

35.4.7 Corretta applicazione DPIA

Verifica a campione:

1. sulla corretta compilazione delle DPIA laddove esistenti,
2. sui trattamenti, al fine di verificare se ne sussistono alcuni che necessitano dell'effettuazione di una DPIA non ancora svolta.

35.5 Il piano delle verifiche sulle misure di sicurezza

Compito specifico del Security IT Manager, nell'ambito della sua attività di auditing, è quello di programmare ed attuare il piano delle verifiche sulle misure di sicurezza, con obbligo di riportare il proprio operato al DPO e al Titolare in apposita relazione.

35.5.1 Verifica catalogo degli asset

Tale piano di verifiche comprende:

1. verifica dell'adeguatezza delle misure generali di sicurezza alla evoluzione delle minacce IT
2. verifica a campione, incrociando diverse fonti, circa la completezza del catalogo degli asset con particolare riferimento alle misure di sicurezza ed al loro collegamento con i trattamenti.

35.5.2 Adeguatezza delle misure di sicurezza

1. Verifica a campione sulle misure di sicurezza associate agli asset/trattamenti e valutazione circa l'adegautezza delle stesse rispetto alle mutate minacce IT,
2. verifica a campione sui comportamenti di strutture interne o fornitori in merito alle procedure previste al fine di limitare i rischi (es. aggiornamento del software, utilizzo di sistemi di identificazione autenticazione e accesso adeguati, verifica che personale che accede ai servizi IT sia correttamente identificato e abbia abbinato il corretto profilo, ecc..)

35.5.3 Risk assessement

Il piano comprende, inoltre, l'effettuazione di risk assessment tesi ad evidenziare le misure adottate, con riferimento ai diversi contesti architetturali e ai diversi asset, valutandone il rischio residuo rispetto alle minacce. Ciò finalizzato all'individuazione di eventuali remediation plan. Per ogni ambito esaminato (data center, sottorete, ecc.) deve essere effettuata una valutazione in merito alla proporzionalità tra livello di rischio residuo e danno che il verificarsi dell'evento lesivo in ambito data protection potrebbe causare (ad esempio un conto è un ambiente che gestisce solo dati amministrativi, altro conto è un ambiente per dati sanitari e di pronto intervento).

35.5.4 Penetration test

Devono, inoltre, essere effettuati test tesi ad individuare i punti di debolezza nell'accesso alle reti, ai sistemi e alle applicazioni, con formulazione di correlati remediation plan.

35.5.5 Verifica della documentazione disponibile

Controllo sulla disponibilità di documentazione e sul relativo livello di aggiornamento rispetto alle reti, ai sistemi, alle applicazioni, alle misure di sicurezza comprensive della disponibilità e continuità del servizio. Verifica a campione della qualità di detta documentazione.

35.5.6 Verifica di situazioni di lock in

Attraverso la verifica della documentazione, delle modalità di gestione dei sistemi, della portabilità degli ambienti da un fornitore ad un altro, da un ambiente ad un altro, viene valutato il grado di lock in del sistema, definibile come grado di libertà del proprietario dei dati e/o delle applicazioni di cambiare fornitore e/o ambiente tecnologico. Occorre che l'amministrazione sia libera da vincoli tesi a precostituire situazioni nelle quali il fornitore o gestore (responsabile) dei sistemi e dei dati, diventi un soggetto vincolante per future e diverse scelte e che sia in grado di evitare la configurazione di situazioni di non continuità nella erogazione dei servizi.

35.5.7 Verifica della effettiva e tempestiva comunicazione di incidenti

Verifica che i gestori dei sistemi abbiano comunicato tempestivamente incidenti con valutazione degli effetti della mancata o tardiva comunicazione. Tali eventi devono essere rilevati e devono essere oggetto di specifica sanzione, oltre che di comunicazione al DPO e al Titolare

36 Processi Ispettivi

Il processo di ispezione generale del Garante Privacy presuppone il necessario coinvolgimento di DPO e Security Manager, che sono tenuti a mettere a disposizione dell'autorità di controllo la documentazione attestante:

1. la compliance organizzativa;
2. la compliance di processo;
3. l'attività continua di monitoraggio;
4. il registro dei trattamenti;
5. il registro degli incidenti.

Qualora l'ispezione riguardi uno o più specifici trattamenti, vengono coinvolti anche il Titolare o suo delegato/i, il Responsabile se esistente, e per ogni trattamento occorre produrre:

1. la registrazione nel registro dei trattamenti:
    a. informazioni generali sul trattamento;
    b. indicazione dei soggetti autorizzati;
    c. gli asset coinvolti;
    d. le misure di sicurezza adottate;
2. il dossier data protection del processo;
3. la segnalazione/ denuncia (se pervenuta):
    a. le informazioni generali;
    b. le azioni poste in essere per contenere il danno nell'immediato;
    c. le azioni di miglioramento della sicurezza e di riduzione del rischio programmate;
    d. le comunicazioni effettuate agli organismi preposti (Garante, autorità giudiziaria) ed eventualmente agli interessati.

37 Indicazioni operative

Al fine di rendere effettivo il processo di compliance occorre realizzare ed avviare un vero e proprio sistema informativo, Information System for Data Protection (IS4DP), caratterizzato dalle seguenti componenti:

1. **Sistema documentale** per la catalogazione dei documenti inerenti il sistema data protection (compliance organizzativa) e per la gestione dei dossier di Data Protection (compliance di processo) e relative procedure per la sua implementazione e gestione;
2. Sistema Registro dei trattamenti connesso con:
   a. il sistema di gestione delle risorse umane e delle strutture organizzative al fine di mantenerlo aggiornato al variare delle strutture, dei responsabili in quanto delegati dal Titolare e degli addetti in quanto autorizzati;
   b. il sistema di gestione degli asset e le relative misure di sicurezza classificabili come "Misure di sicurezza generali", in quanto riferite a tutta l'infrastruttura e "Misure di sicurezza specifiche" in quanto riferite allo specifico trattamento;
   c. il sistema di documentazione di cui al punto precedente, attraverso il riferimento al Dossier Data Protection quale contenitore di tutta la documentazione relativa al processo complessivo di cui quel trattamento costituisce parte;
3. **Sistema di gestione degli incidenti, e monitoraggio misure di sicurezza** con collegamento con il sistema documentale ed i Dossier Data Protection;
4. **Sistema di gestione della DPIA**, con relativi collegamenti con:
   a. catalogo degli asset e relative misure di sicurezza;
   b. dossier data protection;
   c. registro dei trattamenti;
5. Sistema per la gestione del fascicolo del cittadino;
6. Sistema di gestione delle istanze degli interessati in collegamento con:
   a. fascicolo del cittadino;
   b. registro dei trattamenti;
7. **Revisione sistema di gestione degli atti** al fine di intercettare e gestire quegli atti che hanno rilevanza per la compliance al GDPR e costituire o implementare il dossier data protection.

Processo di garanzia dei diritti degli interessati
Linee Guida

1 Scopo del documento

Il presente documento, costituisce linee guida per il processo relativo alla tutela e garanzia dei diritti degli interessati previsto nel GDPR, regolamento europeo 679/2016 sulla Protezione dei dati.

38 Trasparenza e modalità

L'art 12 del Reg. (ue) n. 679/2016, enuncia il principio di trasparenza.

Con tale principio, il Regolamento pone al centro dell'attività compiuta dai soggetti che svolgono il trattamento dei dati, l'accessibilità ad essa da parte dell'interessato, intesa come conoscibilità da parte del soggetto, del suo diritto all'esercizio del controllo sui dati che lo riguardano e degli effetti che i trattamenti possono avere. Tale principio, trova manifestazione sia nelle informazioni obbligatorie di cui agli artt. 13 e 14, che nel riscontro alle richieste presentate ai sensi degli artt. dal 15 al 22.
Il principio di trasparenza, non si limita a un dovere informativo sul trattamento dei dati, esso riguarda anche l'informazione circa le modalità con cui, colui che pone in essere l'attività di trattamento, sia esso Titolare o Responsabile, deve fornire le informazioni al soggetto interessato.

La trasparenza costituisce un elemento indispensabile del trattamento, insieme alla liceità e alla correttezza. La trasparenza è infatti un principio fondamentale del trattamento, oltre che un vero e proprio diritto dell'interessato.

Il principio in questione non riguarda solo i trattamenti, ma è alla base dei rapporti tra il titolare e l'interessato. In tal senso, le informative e le comunicazioni verso l'interessato e quindi l'informativa in particolare, devono essere facilmente accessibili e comprensibili con particolare attenzione quando l'informazione è rivolta ai minori, Devono pertanto essere scritte utilizzando un linguaggio semplice, eventualmente anche tramite grafica e icone, qualora siano forniti in forma elettronica, in modo che gli interessati siano in grado di capirne il contenuto e comprendere come sono trattati i loro dati. L'interessato come sopra evidenziato deve essere in grado di apprezzare anche i rischi che i trattamenti possono comportare, com'è ad esempio nel caso di trattamenti di dati che comprendono flussi transfrontalieri (extra-UE) di dati personali. In tal modo senso anche la valutazione di rischio diventa oggetto dell'obbligo di trasparenza, ed è doveroso che sia svolta e che l'esito sia reso noto sia nei confronti degli interessati che, qualora il trattamento comporti un rischio elevato, all'Autorità di controllo.

Qualsiasi trattamento occulto o segreto deve, quindi, ritenersi illecito. I titolari e i responsabili devono garantire agli interessati che i dati saranno trattati secondo liceità e correttezza. L'obbligo di garantire la trasparenza dei trattamenti grava anche sul Responsabile, ed il Titolare è tenuto a verificare l'adeguamento del Responsabile al principio sopra enunciato, prima di designarne uno.

39 L'informativa

Il principio di trasparenza impone al titolare del trattamento l'adozione di misure appropriate, sia tecniche sia organizzative, per fornire agli interessati tutte quelle informazioni, previste dagli articoli 13 e 14 del regolamento, che spieghino agli interessati le finalità specifiche per le quali sono stati raccolti i loro dati, quali sono le norme, le garanzie e le modalità del trattamento, a quali rischi potrebbero essere esposti, quali sono i loro diritti (articoli 15-22 regolamento, ove applicabili) e come esercitarli.

Di tale obbligo, il titolare può essere chiamato in qualunque momento a renderne conto.

40 Contenuti dell´informativa

I contenuti dell'informativa sono elencati in modo tassativo negli articoli 13, paragrafo 1, e 14, paragrafo 1, del Regolamento. In particolare, il titolare deve sempre specificare:
eI propri dati di contatto e quelli del DPO (Data Protection Officer, figura obbligatoria per i soggetti pubblici); le finalità del trattamento e la base giuridica del trattamento; qualora il trattamento si basi sui legittimi interessi di cui all'art. 6, lett. f), l'indicazione di essi se non è effettuato dall'autorità pubblica nell'esercizio dei suoi compiti; i destinatari o le categoria di destinatari dei dati personali; nonché se trasferisce i dati personali in Paesi terzi o a organizzazioni internazionali, se vi è una decisione di adeguatezza della Commissione o, nel caso di trasferimenti per cui ci sia necessità di adottare mezzi di tutela particolari (art. 46; 47 o 49, 2 comma) attraverso quali strumenti l'indicazione delle garanzie appropriate o opportune e dei mezzi con cui il soggetto può richiedere una copia dei dati nel luogo in cui sono stati resi disponibili. (esempio: si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; si utilizzano BCR di gruppo; sono state inserite specifiche clausole contrattuali modello, ecc.). Inoltre, nel caso di trattamenti di dati personali raccolti presso una fonte diversa dall'interessato (ad es. da altra pubblica amministrazione), applicandosi dunque il disposto ex art. 14 GDPR, andrà specificata la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico (art. 14, comma 2, lett. F).

Il regolamento prevede anche ulteriori informazioni che devono essere fornite all'interessato, in quanto "necessarie per garantire un trattamento corretto e trasparente". Il titolare deve specificare il periodo di conservazione dei dati o, qualora non possa essere definito, i criteri seguiti per stabilire tale periodo di conservazione e il diritto di presentare un reclamo all'autorità di controllo. Se il trattamento comporta processi decisionali automatizzati (quali la profilazione), l'informativa deve specificarlo e deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.

41 Tempi della informativa

L'informativa deve essere data agli interessati sempre prima di iniziare il trattamento.
Nel caso in cui i dati personali non siano raccolti direttamente presso l'interessato *(art. 14 del regolamento)*, l'informativa deve essere fornita entro un termine ragionevole e non oltre può superare 1 mese dalla raccolta dei dati, oppure al momento della comunicazione dei dati a terzi o all'interessato.

Il regolamento fissa i requisiti presupposti per l'esonero dalla informativa: spetta al titolare, in caso di dati personali raccolti da fonti diverse dall´interessato, valutare se la prestazione dell´informativa agli interessati risulti impossibile o comporti uno sforzo sproporzionato.

42 Modalità della informativa

L'informativa deve avere forma concisa, trasparente, intelligibile per l'interessato e deve essere facilmente accessibile; occorre utilizzare un linguaggio chiaro e semplice, e per i minori occorre prevedere informative idonee, scritte in una forma e con un linguaggio comprensibile dagli stessi.

L’informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico, soprattutto nel contesto di servizi online, anche se sono ammessi "altri mezzi", quindi può essere fornita anche oralmente, ma solo se lo richiede l’interessato stesso.

Il regolamento ammette l’utilizzo di icone per presentare i contenuti dell’informativa in forma sintetica, ma solo "in combinazione" con l’informativa estesa; queste icone dovranno essere identiche in tutta l´Ue e saranno definite prossimamente dalla Commissione europea.

43 Modulistica

Modelli di informative per le strutture della Giunta regionale sono disponibili sulla intranet, tra la modulistica relativa alla sezione “Protezione dei dati”.
I modelli contengono le informazioni minime obbligatorie previste dal regolamento, devono essere adattati al caso concreto e completati con le informazioni mancanti, possono essere integrate con contenuti ulteriori, ma i contenuti già previsti nei modelli non possono essere ridotti.

44 Diritti degli Interessati

I paragrafi di seguito riportati contengono la descrizione dei diritti degli interessati a cui il Titolare del trattamento deve dare riscontro nei tempi e con le modalità indicate nel presente documento. Qualora le richieste dell’interessato siano manifestamente infondate o eccessive, per il loro carattere ripetitivo, il titolare può opporre il rifiuto al soddisfacimento delle stesse dimostrandone il carattere eccessivo o infondato.

44.1Diritto di accesso (art.15 regolamento)

L’art. 15 del Regolamento tratta del diritto di accesso dell’interessato. L'interessato ha il diritto di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

1. le finalità del trattamento;
2. le categorie di dati personali in questione;
3. i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
4. i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
5. quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
6. l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
7. il diritto di proporre reclamo a un'autorità di controllo;
8. qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
9. esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato;

10. qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, esistenza di garanzie adeguate relative al trasferimento. Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento, a meno che ciò non costituisca lesione di diritti di terzi. *(Il Considerando n. 63 al Regolamento, precisa che, qualora il Titolare tratti una notevole quantità di dati dell'interessato, può essere richiesto a quest'ultimo di specificare le informazioni o le attività di cui richiede l'accesso)*

44.2 Diritto di rettifica (articolo 16 regolamento)

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

44.3 Diritto alla cancellazione («diritto all'oblio») (articolo 17 regolamento)

L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il Titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

1. i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
2. l'interessato revoca il consenso su cui si basa il trattamento e se non sussiste altro fondamento giuridico per il trattamento;
3. l'interessato si oppone al trattamento per motivi connessi alla sua situazione particolare e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento per finalità di marketing diretto;
4. i dati personali sono stati trattati illecitamente;
5. i dati personali devono essere cancellati per adempiere un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento.

La richiesta di cancellazione può essere respinta se ricorre uno dei motivi seguenti:

1. per l'esercizio del diritto alla libertà di espressione e di informazione;
2. per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
3. per motivi di interesse pubblico nel settore della sanità pubblica;
4. a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, nella misura in cui la cancellazione rischia di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;
5. per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

44.4 Diritto di limitazione (articolo 18 regolamento)

L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:

1. l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;
2. il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
3. benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
4. l'interessato si è opposto al trattamento per motivi connessi alla sua situazione particolare, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

La limitazione del trattamento comporta che il titolare può trattare i dati, oltre che per la conservazione, solo per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.
L'interessato ha diritto ad essere informato circa la revoca della limitazione.

44.5 Diritto di opposizione (articolo 21 regolamento)

L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, compresa la profilazione.
Ciò comporta che il titolare del trattamento debba astenersi dal trattare ulteriormente i dati personali, salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento, che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato, oppure opporsi per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. Qualora i dati personali sono trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione, nella misura in cui sia connessa a tale marketing diretto. Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguardano, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

44.6 Obblighi ulteriori del Titolare

Nel caso di accoglimento delle richieste da parte dell'interessato di rettifica, cancellazione o di limitazione dei dati, il titolare è tenuto ad adottare misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

Di regola, i diritti GDPR sono azionabili per qualsiasi tipo di trattamento. In taluni casi, di seguito sintetizzati, esistono specifiche correlazioni tra le basi giuridiche dei trattamenti ed i diritti azionabili:

45 Modalità esecutive

45.1 Presentazione della richiesta

Le richieste degli interessati possono pervenire unicamente tramite i canali dedicati (casella email urp_dpo@regione.toscana.it per informazioni di carattere generale o mediante Sito web Regione Toscana speciale DPO, " Garanzia diritti dell'interessato". Resta inteso che è onere dell'ente agevolare l'esercizio dei diritti di data protection nei limiti di quanto materialmente possibile, dunque garantendo che tale canale e-mail:

1. Sia indicato in ogni informativa erogata ai sensi degli artt. 13 e 14 GDPR
2. Sia costantemente monitorato, affinché sia garantito il rispetto dei termini di riscontro previsti dal GDPR (30 giorni, prorogabili di ulteriori 2 mesi nei casi di esercizio di diritti di peculiare complessità, documentabile dal Titolare)
3. Sia affiancato da canali di comunicazione, comunque adeguatamente riportati in informativa, non telematici. Ciò al fine di garantire l'esercizio dei suddetti diritti anche da parte di soggetti non muniti di connessione internet, come nel caso di persone meno abbienti, di residenti in aree non coperte da servizi internet o di persone non alfabetizzate dal punto di vista informatico.

Se l'interessato inoltra la richiesta tramite il servizio on-line *"garanzia dei diritti dell'interessato"* lo stesso viene identificato tramite CNS/TS o SPID; il servizio, che guida l'interessato a comporre la richiesta garantisce che siano inserite tutte le informazioni utili a dare immediatamente seguito alla richiesta.
Per le richieste inviate via email, l'interessato potrà scaricare l'apposito modulo dalla pagina web del sito del Titolare, compilarlo ed inviarlo all'indirizzo e.mail indicato allegando, la fotocopia del proprio documento d'identità in corso di validità, oltre all'eventuale documentazione ritenuta necessaria.
Nel caso di invio della richiesta attraverso e.mail o altro canale può presentarsi il problema di dover ricontattare l'interessato per ottenere tutte le informazioni necessarie
In circostanze specifiche, in ossequio al principio di semplificazione dell'esercizio dei diritti dell'interessato, l'ente si riserva di prevedere modalità semplificate di esercizio dei diritti e di identificazione dell'interessato, ad esempio nel caso di unsubscribe a servizi di newsletter informative: in tali casi, conformemente alle linee guida dei Garanti Europei, è possibile procedere all'esercizio del diritto di opposizione direttamente tramite link dedicato contenuto nella newsletter, ovvero procedendo all'identificazione dell'interessato tramite i sistemi di credenziali utilizzate.

Sia che la richiesta pervenga tramite posta elettronica sia attraverso l'uso dell'apposito servizio on-line: viene tenuto traccia delle seguenti informazioni:

1. numero progressivo (per anno);
2. data della richiesta;
3. nominativo dell'interessato;
4. Direzione destinataria della richiesta;
5. Soggetti coinvolti nell'elaborazione della richiesta (interni ed esterni);
6. Stato della richiesta (Inviata/In lavorazione/Conclusa);
7. Data di chiusura della gestione della richiesta.

La richiesta formulata dall'interessato, potrà essere oggetto di richiesta di chiarimenti o integrazioni da parte del DPO o del Titolare. I tempi di soddisfacimento delle richieste avvengono all'interno dei tempi previsti dalla normativa.

45.2Modalità di risposta

Il DPO prende in carico la richiesta e la inoltra al dirigente cui attiene il trattamento in questione per acquisire ogni informazione utile all'elaborazione della risposta. La risposta fornita all'interessato deve essere "intelligibile", concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.
La risposta all'interessato sarà data sullo stesso canale e con gli stessi mezzi con i quali è stata formulata la richiesta. La risposta sarà firmata sia dal Titolare o suo delegato sia dal DPO.
La richiesta di accesso può essere materialmente soddisfatta in vari modi, ad esempio fornendo copia estratta dei dati richiesti, ovvero garantendo, ove possibile, l'accesso a data base (ad esempio nei casi di servizi erogati tramite portali).

45.3 Tempi di risposta

Il termine per la risposta all'interessato è, per tutti i diritti, entro 1 mese, prorogabile di 2 mesi nei casi di particolare complessità e nel caso in cui vi sia la ricezione di numerose richieste. Qualora il termine di un mese fosse prorogato per le esigenze suesposte, deve esserne dato avviso all'interessato, che deve essere informato dei motivi del ritardo entro un mese dal ricevimento della richiesta. Qualora il Titolare non ottemperi alla richiesta dell'interessato, deve informarlo, nel termine di un mese dal ricevimento della stessa, dei motivi del diniego e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale. I tempi si interrompono in caso di richiesta di chiarimenti o integrazioni alla richiesta.
Qualora le richieste dell'interessato siano manifestamente infondate o eccessive, per il loro carattere ripetitivo, il titolare può opporre il rifiuto al soddisfacimento delle stesse dimostrandone il carattere eccessivo o infondato.
I termini devono essere suddivisi internamente in modo che la richiesta possa essere inoltrata ai soggetti che si trattano i dati in outsorcing e che possa pervenire risposta in tempi ragionevoli, tali da consentire di ottemperare alla prescrizione sopra richiamata nei termini di legge.

46 Oneri economici

L'esercizio dei diritti cui fa riferimento la presente procedura è gratuito per l'interessato. Qualora per della richiesta emerge la sua complessità, la molteplicità degli uffici coinvolti nei trattamenti e il coinvolgimento di soggetti esterni all'amministrazioni, è possibile richiedere all'interessato il versamento di un obolo dell'ammontare da definire tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta.

47 Deroghe

Qualora il DPO verifichi la impossibilità o la non applicabilità di una risposta ne informa il Titolare che decide se applicare la deroga alla risposta.
Tali casi sono:

a. impossibilità di identificare l'interessato;
b. carattere manifestamente infondato o eccessivo della richiesta inviata da parte dell'interessato, in particolare per via del carattere ripetitivo della stessa;

Inoltre, come previsto dalla normativa, l'esercizio di uno specifico diritto può essere denegato – dandone comunque debita comunicazione all'interessato - se:

a. la richiesta ricade nel principio di tutela del diritto alla libertà d'espressione e di informazione, incluso il trattamento a scopi giornalistici o di espressione accademica, artistica o letteraria
b. i dati personali sono trattati a fini di ricerca scientifica o storica ,
c. i dati personali sono archiviati a fini meramente statistici,
d. i dati personali sono trattati per finalità di archiviazione nel pubblico interesse.

Nel caso in cui la richiesta debba essere respinta, la risposta dovrà contenere i motivi dell'inottemperanza e le indicazioni sulla possibilità di proporre reclamo all'autorità di controllo o di proporre ricorso giurisdizionale.

48 Controlli

Qualora i dati personali oggetto della richiesta siano trattati da uno o più responsabili del trattamento, il Titolare definisce contrattualmente con i responsabili del trattamento le modalità con le quali essi assicurano l'obbligo di assistere il titolare del trattamento con misure tecniche e organizzative adeguate nel dare seguito alle richieste di esercizio dei diritti dell'interessato, di cui il titolare del trattamento resta legalmente responsabile.

49 Strumenti

La possibilità di garantire canali di comunicazione certi con gli interessati e relativi tempi, risulta indispensabile disporre dei seguenti strumenti:

1. Applicazione web che realizzi il servizio on-line per l'immissione della richiesta da parte dell'interessato, che garantisca certezza dei dati acquisiti e per la gestione del suo completo ciclo di vita tenendo conto delle diverse fasi e relativi tempi;
2. "Fascicolo personale dell'interessato", riportante le banche dati che contengono dati personali e la loro tipologie e caratteristiche;
3. Il Registro dei Trattamenti che consenta il collegamento fra le banche dati, Trattamenti, misure di sicurezza;
4. Una procedura standard che consenta la esportazione di dati presenti nelle banche dati in un formato open, in caso di richiesta di estrazione dei propri dati da parte dell'interessato;
5. Modalità standard di fornire l'informativa all'interno di servizi on-line di raccolta dati

Glossario

Glossario

GDPR: Regolamento Europeo sulla protezione dei dati personali 679/2016 – General Data Protection Regulation

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

Dati biometrici: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

Dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

Dati giudiziari: i dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

Nuovo trattamento: trattamento di dati personali che comporta l'utilizzo di nuove tecnologie o è di nuovo tipo e in relazione al quale il titolare del trattamento non ha ancora effettuato una valutazione d'impatto sulla protezione dei dati, o la valutazione d'impatto sulla protezione dei dati si riveli necessaria alla luce del tempo trascorso dal trattamento iniziale.

Limitazione di trattamento:il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

Profilazione: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

Titolare del trattamento (controller): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

Responsabile del trattamento (processor): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

Contitolare: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che congiuntamente ad altri titolari determina le finalità e i mezzi di trattamento dei dati personali;

Sub responsabile: persona fisica o giuridica designata dal responsabile del trattamento, previa autorizzazione scritta del titolare, che tratta dati personali per conto del titolare del trattamento;

Interessato (data subject): persona fisica identificata o identificabile. Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Consenso dell'interessato: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

Destinatario:la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

DPO: Responsabile della protezione dei dati personali/Data Protection Officer designato dal titolare del trattamento

Security Manager: figura preposta alla gestione e supervisione del processo di Security Incident Management e all'auditing periodico rispetto alle efficienza ed efficacia delle misure adottate.

Responsabile della Conservazione documentale: figura preposta alla gestione e supervisione del processo di conservazione dei documenti (digitali o cartacei).

Autorità di controllo: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR, incaricata di sorvegliare l'applicazione del Regolamento UE 2016/679 al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione. Nel caso Italiano è l'Autorità Garante per la protezione dei dati personali.

Rappresentante: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27 del GDPR, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del regolamento;

Delegato del titolare: il dirigente responsabile della struttura presso la quale si svolgono i trattamenti, cui il titolare Giunta regionale delega l'esercizio delle proprie competenze in materia di protezione dei dati in coerenza con le responsabilità derivanti dalla l.r. 1/2009 e, dove possibile, con la responsabilità del procedimento amministrativo

Responsabile dei sistemi informativi: il dirigente responsabile della struttura deputata a tradurre l'ipotesi di soluzione in macro progettazione e progettazione di dettaglio e successivamente alla messa in esercizio di quanto progettato,

Responsabile sicurezza delle infrastrutture: il dirigente responsabile della struttura deputata a tradurre, in collaborazione con il responsabile dei sistemi informativi, l'ipotesi di soluzione in

macro progettazione e progettazione di dettaglio in riferimento ai servizi infrastrutturali quali sistemi, reti, middleware, ecc..

Security IT Manager/**Responsabile degli Archivi**: il responsabile della struttura deputata a verificare, sia in fase di progettazione sia durante la vita della soluzione, l'adeguatezza delle misure di sicurezza adottate.

Ufficio del DPO: struttura di supporto e consulenza del titolare e sui delegati con un compito specifico di verifica e rilascio di parere non vincolante del dossier data protection che descrive la soluzione in via di adozione, alla luce del GDPR.

Responsabile della sicurezza IT: la persona o la struttura cui è demandato il compito di definire, impostare e gestire le misure di sicurezza IT

Misure di sicurezza: misure tecniche ed organizzative adeguate per garantire un livello di sicurezza dei dati trattati adeguato al rischio.

Anonimizzazione: tecnica di trattamento dei dati personali tramite la quale i dati personali non possano più essere attribuiti a un interessato specifico, nemmeno attraverso l'utilizzo di informazioni aggiuntive.

Pseudonimizzazione: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

Cifratura: tecnica di trattamento dei dati personali tramite la quale i dati personali vengono resi non intellegibili a soggetti non autorizzati ad accedervi.

Violazione dei dati personali (cd. Data breach): la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

Incident management: procedura di gestione degli incidenti IT relativi a dati personali

Data Protection by-design / by-default: l'incorporazione della privacy a partire dalla progettazione di un processo aziendale, con le relative applicazioni informatiche di supporto. La prima introduce la protezione dei dati fin dalla progettazione per caso specifico, la seconda per impostazione predefinita di una pluralità di casi tra loro omogenei.

Processo (process): sequenza di sottoprocessi/attività, poste in essere da persone o soggetti organizzativi diversi (strutture organizzative, enti), tra loro interrelate e finalizzate al conseguimento di un obiettivo comune, che creano valore trasformando delle risorse (input del processo) in un prodotto (output del processo)

Attività: sequenza di operazioni elementari la cui ulteriore scomposizione non sarebbe utile ai fini di un'analisi organizzativo-gestionale di un processo. Ogni attività conduce ad un output sequenza di operazioni elementari la cui ulteriore scomposizione non sarebbe utile ai fini di un'analisi organizzativo-gestionale di un processo. Ogni attività conduce ad un output intermedio preciso, che concorre alla realizzazione dell'obiettivo

Sottoprocesso: parte di un processo che coinvolge un insieme di attività aventi uno specifico obiettivo, il quale però contribuisce al raggiungimento dell'obiettivo più generale del processo. Ogni processo può essere composto da diversi sottoprocessi

Procedimento: pluralità di atti tra loro autonomi, prodotti in un diverso spazio temporale, ma diretti a perseguire lo stesso fine, vale a dire l'emanazione del provvedimento finale.

Procedura: stabilisce "come" un'attività dev'essere svolta, mentre un processo indica "che cosa" dev'essere fatto per raggiungere un risultato o, più propriamente, "chi deve fare che cosa". A differenza dei processi, le procedure non elaborano informazioni, ma descrivono le modalità per elaborare tali informazioni.

Funzioni: insieme di operazioni portate avanti da una singola persona, singola struttura organizzativa o singolo ente finalizzate a supportare uno o più processi

Process owner: figura a cui è affidata la responsabilità dell'intero processo (inclusa la responsabilità del raggiungimento degli obiettivi del processo), che presiede in qualità di coordinatore delle varie funzioni coinvolte. Egli deve garantire il corretto funzionamento del processo nel suo complesso, curandone l'efficacia e l'efficienza.

Categoria delle informazioni: tipologia di dati personali trattati (dati comuni, dati particolari, dati sanitari, dati giudiziari,..) e alla tipologia e numerosità degli interessati, persone fisiche, coinvolti

Lock-In: diminuzione o perdita da parte del titolare della possibilità di gestire i servizi e relativi dati in autonomia senza dover forzatamente ricorrere al soggetto a cui ne ha ceduto la gestione.

DPIA: acronimo di Data Protection Impact Assessment (valutazione di impatto sulla protezione dei dati).

Software "PIA": Applicativo software messo a punto dalla autorità francese per la protezione dei dati (CNIL) per la gestione del processo di Data Protection Impact Assessment.

Dossier DPIA: Insieme delle informazioni raccolte e documentate formalmente durante il processo di Data Protection Impact Assessment fra cui: descrizione del trattamento, conformità al regolamento, obbligo/esenzione DPIA, Analisi dei rischi, eventuale consultazione preventiva, decisioni intraprese, ecc.

Allegati - Data Protection Policy

Elenco Allegati

Nr.	Titolo	Descrizione
1A	Carta Servizi Ufficio DPO	Modalità e tempi per richiedere ed ottenere informazioni, pareri, accesso ai dati, segnlazioni da parte dell' Ufficio del DPO
A	Analisi dei processi	Indicazione metodologica per la analisi e descrizione dei processi
B	Misure di sicurezza	Elencazione delle principali misure di sicurezza da adottare per la protezione di dati personali
C	DPA-TT	Facsimile di data protection agreement per al regolazione dei rapporti data protection fra ***Titolari Autonomi***
D/E	DPA-TR	Facsimile di data protection agreement per al regolazione dei rapporti data protection fra ***Titolari Responsabili e Sub-responsabili***
F	DPA-CTT	Facsimile di Data Protection Agreement per al regolazione dei rapporti Data Protection fra ***Titolari in regime di Contitolarità***.
G	Linee guida Registro Trattamenti	Descrive modalità e contenuti del registro delle attività di trattamento
H	Classificazione dei dati personali	Descrivere le categorie di dati personali e le tipologie degli Interessati
I	Linee guida DPIA	Descrive finalità, contenuti e processo di esecuzione di una analisi di impatto in termini di data protection (***D***ata ***P***rotection ***I***mpact ***A***nalisys)
L	Formulazione di bandi/ contratti/convenzioni/protocolli di intesa	Metodologia per la formulazione di contratti/convenzioni/protocolli d'intesa al fine di individuare i ruoli e responsabilità dei contraenti ai fini del rispetto del GDPR
M/N	Misure di Sicurezza	Criteri e logiche per l'applicazione delle misure di sicurezza.
O	Dossier Data Protection	Descrive finalità, contenuti e processo di formazione ed aggiornamento del dossier data protection, che ha l'obiettivo di mantenere traccia documentale della vita del processo a cui si riferisce

Allegato 1A

Carta dei servizi

Ufficio DPO

1 Scopo del Documento

Lo scopo del presente documento è quello di descrivere i servizi offerti dall'Ufficio del DPO in merito sia a richieste di supporto e consulenza interne all'organizzazione o provenienti da enti esterni, sia a richieste provenienti dall'interessato.

50 La carta dei servizi: Cosa è

La Carta dei servizi è il documento attraverso il quale ciascun soggetto erogatore di servizi assume determinati impegni nei confronti della propria utenza, in relazione ai servizi resi ed informa l'utente in merito alle modalità attraverso le quali gli stessi sono erogati, alle tutele previste e agli standard di qualità.
Oltre ad avere quindi un'importante funzione di informazione e orientamento sui servizi erogati all'utenza, la Carta dei servizi stabilisce i principi e le condizioni per la loro erogazione e impegna formalmente l'Ufficio all'osservanza dei requisiti dichiarati per ciascun servizio.

51 Impegni e principi

La Carta si ispira ai principi di uguaglianza, imparzialità, accessibilità, partecipazione, efficienza ed efficacia, trasparenza, continuità e gratuità. A tal fine, l'Ufficio DPO dell' ente, si impegna ad erogare i propri servizi nel rispetto dei seguenti principi:

a. *Uguaglianza*: gli utenti hanno gli stessi diritti, l'accesso ai servizi e le regole di erogazione degli stessi sono uguali per tutti;
b. *Imparzialità*: il servizio deve essere erogato garantendo parità di trattamento sia tra le diverse aree geografiche, sia tra le diverse categorie o fasce di utenti, che devono essere trattati con obiettività, giustizia ed imparzialità;
c. *Continuità*: l'erogazione del servizio avviene, di norma, con continuità e regolarità durante tutti i giorni lavorativi;
d. *Rispetto dei tempi* : devono essere rispettati i tempi di conclusione per ogni singolo servizio;
e. *Partecipazione*: il diritto alla partecipazione degli utenti (cittadini, dipendenti, imprese, associazioni, enti e agenzie) deve essere sempre garantito. L'utente ha il diritto di accesso alle informazioni che lo riguardano e nel contempo può formulare suggerimenti utili al miglioramento del servizio nonché a presentare reclami e segnalare eventuali disservizi. I diritti di conoscenza, accesso e partecipazione sono garantiti nel rispetto di quanto previsto dalle norme nazionali e regionali attualmente vigenti;
f. *Efficacia ed efficienza*: l'erogazione dei servizi deve essere tale da garantire efficacia ed efficienza, a tal fine sono adottati sistemi utili al monitoraggio delle attività svolte nonché alla rilevazione del grado di soddisfazione degli utenti.

52 Chi è il DPO/RPD

Il regolamento (UE) 2016/679 (GDPR), finalizzato alla protezione dei dati personali, ha introdotto, quale figura di garanzia, il Data Protection Officer (DPO) - in italiano il Responsabile

della protezione dei dati (RPD). Nuova figura, obbligatoria per i soggetti pubblici, deputata a promuovere all'interno dell'organizzazione del titolare la cultura della protezione dei dati personali e chiamata a dare attuazione a elementi essenziali del GDPR quali i principi fondamentali del trattamento, i diritti degli interessati, la protezione dei dati sin dalla fase della progettazione (Data Protection by design) e per impostazione predefinita (Data Protection by default), i registri delle attività di trattamento, la sicurezza dei trattamenti, la notifica e la comunicazione delle violazioni di dati personali.

Il DPO/RPD ai sensi dell'art.39 GDPR è incaricato di svolgere le seguenti funzioni:

a. informare e fornire consulenza al "titolare del trattamento" (o suo delegato) nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR, nonché da altre disposizioni nazionali o dell'Unione relative alla protezione dei dati
b. sorvegliare l'osservanza del GDPR, di altre disposizioni nazionali o dell'Unione relative alla protezione dei dati nonché delle politiche del titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c. fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del GDPR;
d. cooperare con l'Autorità di Controllo;
e. fungere da punto di contatto con l'Autorità di Controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del GDPR ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;

In Regione Toscana il DPO è stato nominato con DGR n.325 del 3 aprile 2018 e si è ritenuto di affidargli anche i seguenti compiti:

a) definire un piano di azioni per la piena applicazione del GDPR e della normativa di riferimento per la Giunta regionale, avvalendosi delle competenti strutture delle Direzioni, in relazione ai trattamenti di cui sono responsabili;
b) definire un piano di azioni per la piena applicazione del GDPR e della normativa di riferimento per ciascuno degli Enti e Agenzie di cui sopra, avvalendosi delle competenti strutture di ciascun Ente in relazione ai trattamenti di cui sono responsabili.

53 Ufficio del Data Protection Officer/Responsabile Protezione Dati

L'Ufficio è stato istituito con decreto del Direttore OSI n. 5264 del 13 aprile 2018, che gli ha ascritto le seguenti competenze:

1. Funzioni di responsabile della protezione dei dati (DPO/RPD) ai sensi del Regolamento UE 2016/679, anche per la struttura operativa del Consiglio regionale e degli enti dipendenti. In tale veste: fornisce consulenza al titolare del trattamento o ai responsabili del trattamento dei dati in ordine agli obblighi derivanti dal regolamento e dalla normativa di riferimento; sorveglia l'osservanza del regolamento e delle altre disposizioni in materia da parte delle strutture del titolare; collabora nello svolgimento della valutazione di impatto sulla protezione dei dati; coopera~~zione~~ e funge da punto di contatto con l'Autorità di Controllo,

2. Definizione di indirizzi, linee guida e azioni per l'attuazione della normativa di riferimento in materia di protezione dei dati personali per la Giunta, il Consiglio e gli enti dipendenti.
3. Regolazione e gestione delle attività relative alla protezione dei dati personali, ivi compresa la tenuta del registro delle attività di trattamento della Giunta regionale.
4. Rete Referenti Sistema Privacy delle strutture di vertice della Giunta.
5. Progetti di cybersecurity nell'ambito del Piano Nazionale Industria 4.0.
6. Coordinamento dei progetti di cybersecurity nel sistema regionale e promozione della sicurezza by design nelle soluzioni di information tecnology.

54 Organizzazione dell'Ufficio DPO

Attualmente l'Ufficio DPO/RPD risulta composto come segue:

1. 1 dirigente, con funzioni di DPO
2. 1 funzionario sistemi informativi e tecnologie esperto
3. 1 funzionario amministrativo con competenze giuridiche
4. 1 funzionario amministrativo addetto a funzioni di audit e monitoraggio
5. 1 Assistente amministrativo
6. 1 Assistente programmazione

La sede è posta in Via di Novoli 26, Firenze, Pal. A, 2° piano

55 Utenti

Con la presente Carta dei servizi l'Ufficio RPD si rivolge in primo luogo a cittadini, dipendenti, altri soggetti dell'amministrazione regionale, nonché titolari del trattamento (GR, Enti e Agenzie Regionali) e autorità di controllo. La Carta è inoltre rivolta a coloro che agiscono a supporto degli stessi (tutori legali, delegati, associazioni di categoria, liberi professionisti…)

56 Servizi erogati

SERVIZI RIVOLTI AGLI INTERESSATI							
Servizio	***Descrizione***	***Riferimenti normativi***	***Durata massima gg***	***Utenti***	***Attori coinvolti***	***Atto conclusivo***	***Termini di decorrenza***
Richiesta informazioni (generica)	Richieste di informazione sull'applicazione della normativa in materia di protezione dei dati personali o su uno specifico trattamento	- GDPR - D.Lgs. 196/2003 modificato dal D.Lgs. 101/2018 - altre disposizioni in materia di protezione dei dati	Da 7 a 10 gg, a seconda della complessità di quanto richiesto, salvo interruzione del termine dovuto a richieste di integrazioni	Tutti	URP – Ufficio DPO – referenti DPO di drz/enti/agenzie - soggetti esterni (responsabili del trattamento) competenti nella materia oggetto della richiesta	Risposta scritta del funzionario dell'Ufficio DPO assegnatario della richiesta	Dalla data del protocollo in arrivo della richiesta di informazioni
Esercizio dei Diritti	Richiesta dell'interessato rivolta ad avere conferma che vi sia o meno in corso un trattamento di dati personali che lo riguarda e di ottenere l'accesso ai suoi dati, nonché ad esercitare i diritti sugli stessi, quali rettifica, cancellazione,	Artt. 15-22 GDPPR	Prima possibile e comunque entro 30 gg, salvo interruzione del termine dovuto a richieste di integrazioni e chiarimenti	Cittadini/dipendenti/ fornitori/collaboratori	URP – Ufficio DPO – referenti DPO di drz/enti/agenzie - strutture titolari del trattamento - soggetti esterni (responsabili del trattamento)	Risposta scritta del DPO	Dalla data del protocollo in arrivo della richiesta relativa all'esercizio dei diritti dell'interessato

	limitazione del trattamento ed opposizione		Il termine può essere prorogato di 2 mesi tenuto conto della complessità e del numero delle richieste				
Segnalazioni	Reclamo relativo ad un trattamento ritenuto illecito, illegittmo o non conforme alla normativa sulla protezione dei datai personali	- GDPR - D.Lgs. 196/2003 modificato dal D.Lgs. 101/2018 - altre disposizioni in materia di protezione dei dati	Prima possibile e comunque entro 30 gg, salvo interruzione del termine dovuto a richieste di integrazioni e chiarimenti Il termine può essere prorogato di 2 mesi tenuto conto della complessità e del numero delle richieste	Tutti	URP – Ufficio DPO – referenti DPO di drz/enti/agenzie - strutture titolari del trattamento - soggetti esterni (responsabili del trattamento)	Risposta scritta del DPO	Dalla data del protocollo in arrivo della segnalazione
SERVIZI RIVOLTI ALL'AUTORITA' DI CONTROLLO							
Servizio	***Descrizione***	***Riferimenti normativi***	***Durata massima gg***	***Utenti***	***Attori coinvolti***	***Atto conclusivo***	***Termini di decorrenza***

Richieste del Garante per la protezione dei dati personali	Richieste di informazioni che l'autorità di controllo fa nell'esercizio dei propri poteri	- GDPR - D.Lgs. 196/2003 modificato dal D.Lgs. 101/2018	Nei termini indicati dall'autorità	Autorità di controllo	URP – Ufficio DPO – referenti DPO di drz/enti/agenzie - strutture titolari del trattamento - soggetti esterni (responsabili del trattamento)	Risposta scritta del DPO	Dalla data del protocollo in arrivo della richiesta
SERVIZI RIVOLTI AGLI UTENTI							
Servizio	***Descrizione***	***Riferimenti normativi***	***Durata massima gg***	***Utenti***	***Attori coinvolti***	***Atto conclusivo***	***Termini di decorrenza***
Registro trattamenti	Definizione dei contenuti del Registro; controllo e monitoraggio dell'aggiornamento del Registro da parte delle strutture dell'organizzazione del titolare del registro dei trattamenti informatizzato; produzione del registro cartaceo	- Art. 30 GDPR	Produzione del Registro cartaeo entro l'ultimo del mese; Registro informatizzato aggiornato ad evento	GR/CR/Enti/Agenzie	Ufficio DPO – referenti DPO di drz/enti/agenzie - strutture titolari del trattamento	Registro dei trattamenti (cartaceo e informatizzato)	Registro informatizzato sempre online; Regisro cartaceo dal 1° del mese in corso-
Segnalazioni incidente/ Data breach	Procedura volta a registrare, e se ricorrono le condizioni, a notificare all'autorità di controllo e agli interessati coinvolti, una violazione di dati personali	- Artt. 33-34 GDPR	Entro 72 ore dalla violazione accertata	referenti di direzione, referenti enti, responsabili sistemi informativi, fornitori di servizi GR/CR/Enti/Agenzie	Ufficio DPO – referenti DPO di drz/enti/agenzie - strutture titolari del trattamento - soggetti esterni (responsabili del trattamento) - Security manager - Responsabili sistemi informativi	- Verbale DPO; - notificazione del DPO all'Autorità di controllo; - Comunicazione del DPO agli	dal momento in cui il titolare ha conoscenza dell'avvenuta violazione

					Resp. Sicurezza infrastruttura Responsabile Archivi - Resp Patrimonio	interessati	
DPIA	Processo di analisi dell'impatto di un trattamento sui diritti e le libertà degli interessati volto a valutare il livello di rischio che il trattamento stesso può comportare sulla protezione dei dati personali degli interessati	Artt. 35-36 GDPR	Da 7 a 14 gg, a seconda della complessità di quanto richiesto, salvo interruzione del termine dovuto a richieste di integrazioni	GR/CR/Enti/Agenzie	Ufficio DPO – referenti DPO di drz/enti/agenzie - strutture titolari del trattamento - soggetti esterni (responsabili del trattamento) - Security manager - Responsabili sistemi informativi Resp. Sicurezza infrastruttura Responsabile Archivi Resp Patrimonio	Parere DPO	Dalla data di richiesta di avvio del processo
Pareri	Richieste di informazione e consulenza da parte delle strutture che eseguono i trattamenti in merito agli obblighi derivanti dal GDPR	- GDPR - D.Lgs. 196/2003 modificato dal D.Lgs. 101/2018 - altre disposizioni in materia di protezione dei dati	Da 7 a 30 gg, a seconda della complessità di quanto richiesto, salvo interruzione del termine dovuto a richieste di integrazioni	Referenti di direzione per la GR e enti CR/Enti/Agenzie	URP – Ufficio DPO – altre strutture/enti/agenzie/soggetti esterni (responsabili del trattamento) competenti nella materia oggetto del parere	Parere scritto del DPO	Dalla data del protocollo in arrivo della richiesta di parere

ATTIVITA' SPECIFICHE DELL'UFFICIO DPO							
Servizio	***Descrizione***	***Riferimenti normativi***	***Durata massima gg***	***Utenti***	***Attori coinvolti***	***Atto conclusivo***	***Termini di decorrenza***
Attività di audit	Processo di valutazione volto a verificare la conformità alla normativa sulla protezione dei dati personali dei trattamenti posti in essere nell'organizzazione del titolare	- art. 39 GDPR	Entro 7 gg , salvo impedimenti organizzativi degli uffici coinvolti	GR/CR/Enti/Agenzie	Ufficio DPO – referenti DPO di drz/enti/agenzie – struttura del titolare soggetto ad audit	Verbale Ufficio DPO	Dalla data di avvio dell'audit
Relazione al Titolare	Relazione sull'applicazione e la conformità della normativa in materia di protezione dati personali e stato dell'arte nell'organizzazione del titolare	- GDPR - D.Lgs. 196/2003 modificato dal D.Lgs. 101/2018 - altre disposizioni in materia di protezione dei dati	Entro 31 marzo	GR/CR/Enti/Agenzie	Ufficio DPO	Relazione DPO	Relativo all'anno precedente

57 Come accedere al servizio

Il canale di contatto messo a disposizione di tutti gli utenti attualmente è il seguente indirizzo email: urp_dpo@regione.toscana.it e servizi web nel sito della Regione Toscana, speciale Data Protection/privacy.
Nessuno spostamento è quindi richiesto né rispettare orari di apertura o chiusura. Il servizio accessibile h24 per 365 giorni all'anno.

58 Suggerimenti e reclami

Ogni utente può inviare suggerimenti di miglioramento del servizio o reclami per segnalare difformità tra quanto previsto dalla Carta dei servizi e quanto effettivamente erogato.
Suggerimenti e reclami possono essere presentati via e-mail all'indirizzo:
urp_dpo@regione.toscana.it Possono altresì essere presentati in forma scritta, eventualmente utilizzando l'apposito modulo disponibile presso gli uffici regionali. Ad ogni reclamo scritto sarà data risposta entro 30 giorni presso l'indirizzo indicato dall'utente.
La raccolta di suggerimenti e reclami ha lo scopo di favorire il miglioramento dei servizi. Per questo, occorre che il suggerimento e il reclamo siano presentati su un documento in cui compaiano anche i dati di contatto del mittente, allo scopo di facilitare il feedback da parte della struttura.

59 Customer satisfaction

L'Ufficio Responsabile Protezione Dati periodicamente può trasmettere ai suoi utenti un apposito questionario volto a monitorare la qualità del servizio. La partecipazione è su base volontaria ed i dati sono anonimi.
I risultati saranno pubblicati sul sito web della Regione con la massima trasparenza e tutela della privacy.

Allegato A

Analisi e descrizione Processi
Metodologia e strumenti

1 Scopo del documento

Il presente documento illustra la metodologia per descrivere i processi dell'Ente ed ha l'obiettivo di rappresentare un quadro di riferimento della metodologia da applicare per la mappatura dei processi, anche ai fini della piena attuazione del Regolamento Europeo nr. 679/2016 (General Data Protection Regulation meglio noto come GDPR).

60 Premessa

La descrizione del Processo è elemento iniziale e basilare per l'attuazione del principio di Data Protection by Design in ottemperanza a quanto disposto come uno dei principi di base dal GDPR.
In estrema sintesi la descrizione del processo che si intende mettere in atto con una proposta di legge, con un regolamento, con una delibera o con un decreto, sarà finalizzata ad individuare i soggetti coinvolti in quel processo, le attività o i sottoprocessi in capo ai diversi soggetti e di conseguenza i trattamenti dati che questi sono chiamati ad effettuare.
Risulta evidente che la granularità, il livello di dettaglio, di descrizione del processo saranno adeguati alle diverse tipologie di documenti, atti istitutivi di quel processo.
In fase di proposta di legge il livello di descrizione sarà ovviamente a livello macro, a livello di descrizione relativo ad un decreto attuativo il dettaglio potrà e dovrà essere maggiore. Occorre prendere atto che una legge regionale finalizzata ad esempio al ridisegno del sistema lavoro, o la progettazione di dettaglio di un sistema informativo costituiscono dei progetti (Design) che prefigurano nuovi processi e trattamenti dati che devono fin dalla loro ideazione, farsi carico delle problematiche inerenti il trattamento di dati personali.

61 Concetto di Processo

Un processo è una sequenza di sottoprocessi/attività tra loro interrelate e finalizzate al conseguimento di un obiettivo comune, che creano valore trasformando delle risorse (input del processo) in un prodotto (output del processo)
Elementi del processo
Si possono individuare quali principali elementi di un processo:

a) **Input:** fattori fisici o informativi acquisiti all'esterno o da altri processi, necessari all'avvio del processo;
b) **Output:** prodotto del processo che è destinato al destinatario;
c) **Risorse:** capacità umane e tecnologiche necessarie per svolgere le attività e prendere le decisioni (include anche la definizione dei ruoli e del potere decisionale dei diversi attori);
d) **Logiche di gestione:** logiche di base per coordinare le attività, prendere le decisioni e regolare l'avanzamento del processo;
e) **Fasi:** insiemi di attività e decisioni che, interagendo tra loro, consentono la realizzazione dell'output;
f) **Interdipendenze:** legami logici e di precedenza tra le fasi (attività e decisioni);
g) **Controlli:** dati ed informazioni in ingresso che forniscono norme, regole o procedure;
h) **Eventi:** situazioni che condizionano il flusso del processo;
i) **Vincoli:** regole, istruzioni ed informazioni che influenzano le attività che compongono il processo.

62 Metodologia per la mappatura dei processi

La mappatura dei processi consiste nell'applicazione di una metodologia formalizzata per l'identificazione e la modellazione dei processi.
Con la mappatura si rappresentano gli elementi che compongono un processo: gli input e gli output del processo, le singole attività e le relazioni tra di esse, i soggetti che le attuano e le interfacce esistenti tra gli stessi e, inoltre, i punti di decisione e le alternative che fanno sì che un processo si sviluppi in una direzione piuttosto che in un'altra.
In tal modo si identifica e si documenta ogni processo, fornendo un'evidenza oggettiva e che non possa essere fraintesa, consentendo di:

a) comprendere ciò che realmente viene fatto;
b) Individuare i soggetti organizzativi coinvolti ed i loro ruoli
c) esplicitare le interdipendenze esistenti fra i soggetti organizzativi coinvolti, tra le attività, anche se queste vengono svolte da funzioni organizzative distinte o da enti diversi;
d) condividerne in modo sintetico la conoscenza.

Le evidenze dell'intervento di mappatura sono la base per effettuare la successiva analisi del processo e forniscono il supporto documentale per contribuire a motivarne le conclusioni e le scelte conseguenti.

Le fasi della metodologia

La metodologia da applicare per la mappatura è articolata in 2 macrofasi, in sequenza:

1) Descrizione testuale del processo
2) Rappresentazione grafica del processo

La macrofase 1 consiste nella raccolta delle informazioni necessarie a censire tutti gli elementi che compongono il processo, descrivendo il funzionamento del processo stesso in modo coerente dal punto di vista logico-causale. E' il presupposto per lo sviluppo efficace della macrofase 2.
Il livello di dettaglio di tale descrizione dipenderà dal livello di maturazione della progettazione di impianto e realizzazione del processo.
La rappresentazione grafica, mediante l'uso di specifici simboli secondo uno schema strutturato condiviso, esprime sinteticamente i soggetti le attività o loro raggruppamenti in sottoprocessi, informazioni e risorse coinvolte e indirizza verso una più immediata lettura, decodifica e comprensione del contenuto del processo stesso.

La realizzazione sequenziale e coordinata delle 2 macrofasi consente una maggiore capacità di analisi del processo mappato, tanto in sede di prima analisi che in occasione degli approfondimenti successivi, ai fini delle eventuali revisioni e delle scelte per il miglioramento.
Per ogni macrofase in cui si articola la metodologia è stato predisposto uno specifico strumento applicativo corrispondente, così come riepilogato nella tabella seguente.

macrofase metodologia	strumento applicativo

Descrizione testuale del processo	Scheda processo
Rappresentazione grafica del processo	Diagramma di flusso interfunzionale

63 Strumenti per la mappatura di un processo

63.1Descrizione testuale: Scheda processo

Per la macrofase di descrizione testuale del processo è predisposto per ogni processo un documento chiamato *Scheda Processo* in cui sono individuati e descritti gli elementi che compongono il processo.
La Scheda processo è articolata in 2 sezioni:

1) *Inquadramento*, in cui si devono riportare le informazioni necessarie per l'inquadramento del processo, per ogni argomento richiesto, laddove applicabile;
2) *Sequenza e descrizione*, dove vanno elencati i sottoprocessi/attività che compongono il processo in sequenza cronologica dall'inizio alla fine del processo, e indicate le *categorie di informazioni* richieste per ogni attività, laddove applicabili.

La struttura delle 2 sezioni è di seguito riportata.

Sezione 1 – Inquadramento

INQUADRAMENTO GENERALE DEL PROCESSO	
CODICE	Inserire un codice che identifica il processo
REVISIONE	inserire la revisione (es. Rev.00)
DATA EMISSIONE	Inserire la data di emissione o della revisione della scheda
PROCESSO	Inserire nome del processo
OBIETTIVO	Descrivere la mission, lo scopo del processo
MACROPROCESSO	Inserire nome del macroprocesso (di cui fa parte il processo) se esistente
PROCESS OWNER	Inserire chi ha la responsabilità del processo
PROCESS MANAGER	Inserire chi lo gestisce operativamente (può coincidere con il process owner)
SOGGETTI COINVOLTI	Inserire tutti i soggetti organizzativi diversi coinvolti nel processo

Sezione 2 – Inquadramento
La sezione 2 prevede per ogni singolo sottoprocesso/attività che compone il processo sia riportata in una corrispondente riga, da compilare in riferimento agli argomenti riportati rispettivamente in 9 colonne.

Informazioni relative alla descrizione del sottoprocesso/attività e alla responsabilità correlata Colonne 1 – 3:

Sottoprocesso/attività: Denominazione del sottoprocesso/attività
Descrizione: Descrizione sintetica degli obiettivi delle finalità e dei risultati del sottoprocesso/attività
Soggetto organizzativo competente: Individuare il soggetto organizzativo (struttura, ente,) a cui è affidata la competenza di esercizio di quel sottoprocesso/attività

Informazioni relative all'input del sottoprocesso/attività
Colonne 4-5:
Input : Descrizione dei dati/documenti che innescano il sottoprocesso/attività
Soggetto organizzativo (Input): Soggetto Organizzativo sorgente dei dati/documenti
Informazioni relativa alla tipologia di dati trattati e ai vincoli normativi che disciplinano l'attività Colonne 6– 7:
Categorie informazioni trattate: Riguardano la sintetica descrizione delle categorie dei dati in ingresso riferiti sia ai dati personali sia agli interessati coinvolti nel processo
Leggi, e norme : Leggi e norme che definiscono gli ambiti di competenza entro i quali si muove il soggetto competente

Informazioni relativa all'output del sottoprocesso/attività
Colonne 8-9
Output: Descrizione dei dati/documenti che produce il sottoprocesso/attività
Soggetto organizzativo (Output): Soggetto Organizzativo destinatario dei dati/documenti

63.2Scheda descrittiva riepilogativa del processo

Processo: -- Denominazione Processo. --

Sottoprocesso /attività	Descrizione	Soggetto organizzativo competente	Input	Soggetto organizzativo (Input)	Categorie informazioni trattate	Leggi, e norme	Output	Soggetto organizzativo (Ouput)
Indicare il nome del sottoprocesso/attività	Descrivere sinteticamente il sottoprocesso/ attività in termini di finalità	Individuare il soggetto organizzativo (struttura, ente,) a cui è affidata la competenza di esercizio di quel sottoprocesso/attività	Descrizione dei dati/documenti che innescano il sottoprocesso/attività	Soggetto Organizzativo sorgente dei dati/documenti	Riguardano la sintetica desrizione delle categorie dei dati in ingresso	Leggi e norme che definiscono gli ambiti di competenza entro i quali si muove il soggetto competente	Descrizione dei dati/documenti che produce il sottoprocesso/attività	Soggetto Organizzativo destinatario dei dati/documenti

64 Rappresentazione grafica: Diagramma di flusso interfunzionale

Per la macrofase di rappresentazione grafica del processo va utilizzato per ogni processo il *Diagramma di flusso interfunzionale*.
Con tale strumento si rappresentano graficamente – attraverso una simbologia predefinita e condivisa - gli elementi che compongono il processo, in base a quanto identificato e descritto nella corrispondente Scheda Processo.
In particolare, questo diagramma permette di riportare in uno stesso grafico le informazioni tipiche di un tradizionale diagramma di flusso e – in aggiunta - di identificare i soggetti coinvolti (unità organizzative e/o enti esterni).

Il diagramma di flusso interfunzionale consente di:

a) fornire una visibilità immediata della sequenza delle attività che compongono il processo;
b) indicare le relazioni tra le attività che compongono un processo aziendale e le unità organizzative che ne sono responsabili;
c) scomporre il processo in fasi, singole attività e decisioni da prendere, attribuirle alle unità organizzative e ai ruoli che intervengono nelle diverse fasi del processo e identificare la sequenza logica delle stesse attività.

Permette di rappresentare i tre livelli di un processo di un Ente:

a) livello *private*, ovvero i processi interni all'Ente;
b) livello *abstract*, quello delle relazioni con l'esterno;
c) livello *global*, cioè le interazioni tra Enti diversi e/o tra diversi settori di uno stesso Ente.

Per la rappresentazione grafica sono previste una struttura del diagramma e una simbologia da applicare.

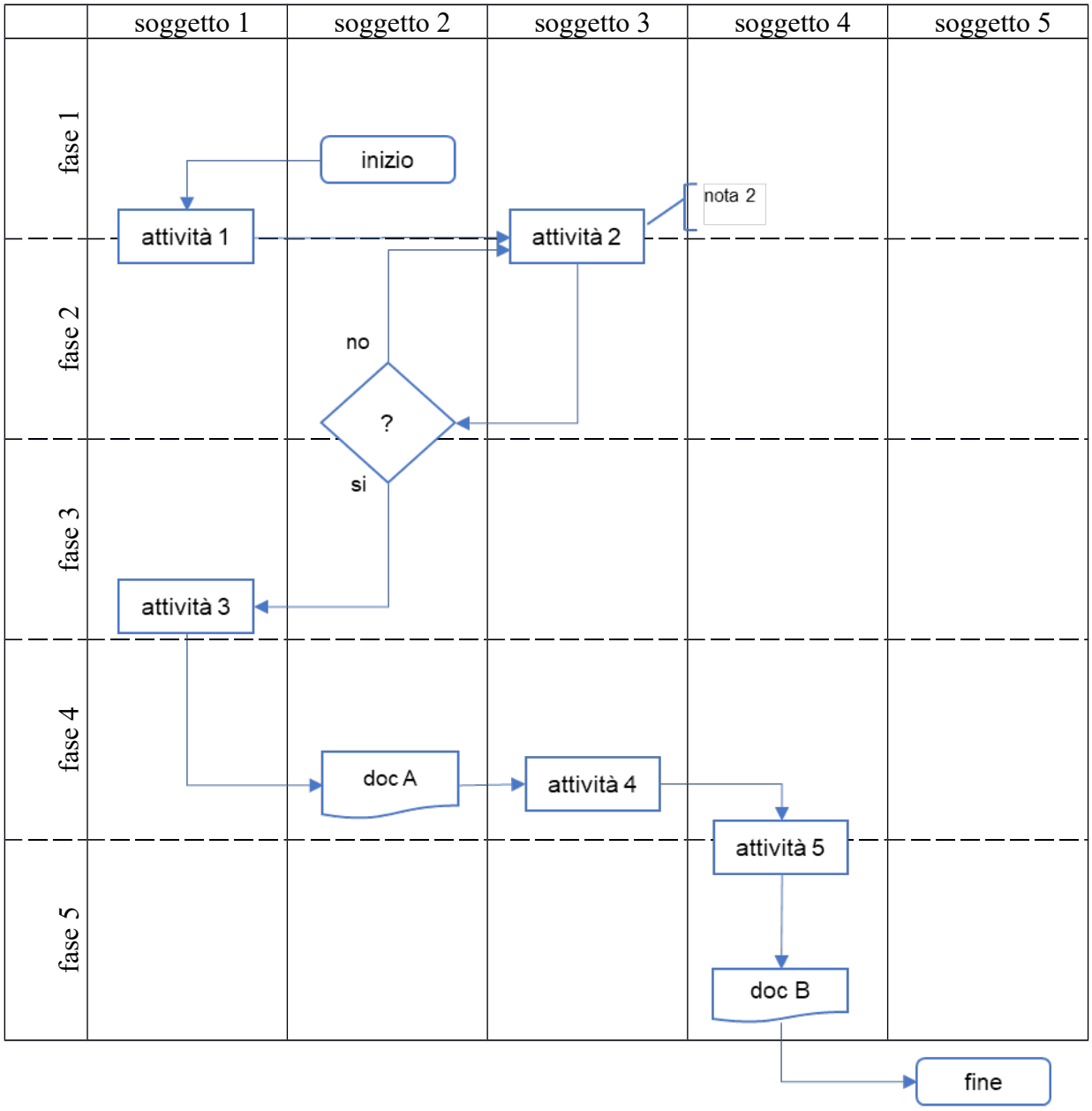
La struttura del diagramma è caratterizzata dai seguenti elementi:
1) le unità organizzative e/o gli enti (soggetti coinvolti), riportate sull'asse orizzontale;
2) le eventuali fasi, entro cui possono essere rappresentate le attività che compongono il processo, indicate sull'asse verticale;
3) le attività, rappresentate all'interno di rettangoli e tra loro collegate da frecce direzionali;
4) le decisioni da compiere, rilevate all'interno di rombi, dai quali si dipanano percorsi alternativi in relazione alla decisione presa;
5) gli strumenti utilizzati/elaborati (ad es. documenti).

La simbologia è riepilogata nella tabella di seguito riportata.

Simbolo	Elemento rappresentato	Descrizione
	Inizio / fine	Rettangolo con angoli smussati Rappresenta l'attività che dà il via e quella che conclude il processo o una parte di esso
	Attività	Rettangolo Rappresenta l'attività che si compie all'interno del processo
	Punto di decisione	Rombo Rappresenta un punto in cui si prende una decisione (in riferimento ad azioni quali verifica, controllo o approvazione). Al suo interno è posta una domanda che richiede la risposta "si" o "no"
	Documento	Rettangolo con ondina Rappresenta la produzione di un documento
	Direzione del flusso e legame tra le attività	Freccia Rappresenta l'indicatore della direzione del flusso
	Annotazioni	Linea con parentesi quadra che racchiude testo Fornisce informazioni aggiuntive ad integrazione della rappresentazione grafica

A titolo illustrativo, si riporta un esempio di diagramma di flusso inter-funzionale secondo la struttura e la simbologia sopraindicate.

cod identificativo processo	nome processo



Allegato B

Misure di Sicurezza per la Data Protection

Linee guida

1 Scopo del documento

Lo scopo del presente documento è di fornire una linea guida in merito alle principali categorie di misure per la sicurezza, per il Responsabile della sicurezza, gli specialisti di sicurezza e per il Security Manager al fine delle procedure di valutazione dell'efficacia delle contromisure esistenti (assessment) ma anche per valutare l'introduzione di ulteriori contromisure a protezione di trattamenti particolarmente critici durante la valutazione di impatto o la rilevazione di incidenti.

65 Premessa

Un processo di analisi dei rischi, sia in ambito SGSI (*Sistema di Gestione della Sicurezza delle Informazioni)* sia di DPIA (*Data Protection Impact Assessment*), una volta conclusa la fase di valorizzazione delle vulnerabilità e minacce, porta conseguentemente alla valorizzazione delle contromisure esistenti.
L'associazione di minacce e contromisure esistenti consente a questo punto di determinare il rischio effettivo che sarà confrontato con un valore di rischio accettabile, precedentemente definito in associazione fra il Titolare e il DPO.
Qualora il valore di rischio sia entro la soglia di accettabilità il trattamento potrà essere definito sufficientemente sicuro e si potrà procedere alla formalizzazione dei risultati in ambito SGSI e/o DPIA.
Nel caso in cui invece il valore di rischio residuo risulti sopra la soglia di accettabilità si dovrà procedere a rivedere le contromisure applicate, alzando il livello di implementazione delle contromisure esistenti oppure introducendo nuove contromisure più efficaci a protezione del trattamento analizzato.

66 Sinergia del sistema di protezione

Per rendere efficace ed efficiente il *Processo di Gestione della Sicurezza delle Informazioni*, l'approccio all'Information Security deve essere un lavoro comune, che implica la partecipazione ed il supporto di tutti gli attori interni, integrata anche con la partecipazione consapevole di fornitori e soggetti esterni.
Questo approccio integrato permetterà di ottenere un sistema di protezione globale ed uniforme nei vari ambiti tecnologici, logistici ed organizzativi di Regione Toscana. La mancanza, o la non applicazione, di criteri di riferimento, che indirizzino tutte le funzioni su quanto di loro competenza nel processo di costruzione della sicurezza determina una disomogeneità del *Sistema di Gestione della Sicurezza delle Informazioni.* Di conseguenza, la presenza di discontinuità nel livello di protezione costruito su un sistema/servizio, vanifica taluni controlli di sicurezza introdotti, che di per sé innalzerebbero il livello di sicurezza.
Per una gestione efficace della sicurezza delle informazioni, si ritengono importanti i seguenti fattori:

a. la politica di sicurezza delle informazioni e le attività che riflettono gli obiettivi gestionali in essa contenuti;

b. l'approccio al modello di gestione della sicurezza delle informazioni coerente con la cultura dell'ente;
c. il supporto visibile della Direzione Generale dell'Ente;
d. la buona comprensione dei requisiti di sicurezza, valutazione e gestione dei rischi;
e. la divulgazione efficace dei principi della sicurezza delle informazioni alle risorse coinvolte in tutti i processi;
f. una distribuzione e condivisione ai soggetti interessati delle informazioni importanti così che ogni attore del sistema possa contribuire a garantire la sicurezza delle informazioni;
g. la garanzia di addestramento e formazione inerenti la sicurezza delle informazioni;
h. un sistema di gestione basato sul modello PDCA *(Plan – Do – Check – Action)* a garanzia di un presidio continuo ed efficace degli aspetti di Sicurezza in ottica di miglioramento continuo;
i. un sistema di misura per valutare le prestazioni del sistema di gestione implementato nonché strumenti di raccolta dei suggerimenti.

67 Fonti per l'individuazione dei controlli di Sicurezza

I requisiti di sicurezza del sistema informativo sono identificati ed aggiornati mediante il ricorso a tre fonti principali:

a. la valutazione dei rischi per il sistema informativo. Questa fonte consente di individuare le minacce, valutare la vulnerabilità e la probabilità di accadimento delle minacce oltre a stimarne l'eventuale impatto;
b. i requisiti legali, prescritti da leggi e normative cogenti fra cui in particolare il Regolamento Ue 679/16, i modelli organizzativi e regolamenti interni derivanti dall'applicazione di leggi e normative cogenti, normative e linee guida facoltative (es. ISO 27001), vincoli contrattuali;
c. una specifica serie di principi, esperienze, best practice, elaborazioni dello stato dell'arte ed obiettivi per il trattamento dei dati all'interno dell'ente.

68 Misure di sicurezza generali (SGSI)

Fermo restando che l'applicazione di specifici controlli di sicurezza è soggetta alle buone prassi riportate all'interno del precedente paragrafo fra cui in primis l'analisi dei rischi) esistono comunque delle classi di contromisure da cui un'organizzazione complessa e articolata quale Regione Toscana non può prescindere per una realizzazione di un sistema di gestione della sicurezza delle informazioni efficace. In altre parole, è difficilmente immaginabile un SGSI in grado di garantire una buona protezione in ambito Data Protection by Default senza l'applicazione di buona parte dei controlli di sicurezza di seguito trattati.
Le misure di Sicurezza di un buon sistema di gestione della sicurezza delle informazioni in ottica di Data Protection, si possono rappresentare e sviluppare secondo i seguenti capisaldi:

1. Sicurezza delle Identità
2. Sicurezza dei Dispositivi di accesso
3. Sicurezza delle Reti

4. Sicurezza dei Sistemi
5. Sicurezza Organizzativa
6. Sicurezza Fisica
7. Disaster Recovery e continuità operativa

68.1Sicurezza delle Identità

La sicurezza delle identità e degli accessi includono tutte le misure di sicurezza (organizzative, logiche e fisiche) volte a garantire - in maniera univoca - l'identità di un soggetto (persona fisica) accedente ad informazioni digitali e/o cartacee. Tali misure devono garantire inoltre un'associazione certa e tracciabile nel tempo fra l'identità personale del soggetto e tutte le sue credenziali di accesso (logiche o fisiche) all'informazione.

68.2Sicurezza dei Dispositivi di Accesso

La sicurezza dei dispositivi di accesso è volta a garantire la sicurezza di tutti i dispositivi (pc, smartphone, tablet, ecc) che consentono ad un soggetto (identità) di poter accedere ad una informazione digitale o cartacea visualizzandola, trasferendola e/o memorizzandola in locale (sia sul dispositivo usato per accesso all'informazione sia su dispositivi di memoria removibili).

68.3Sicurezza delle Reti

La sicurezza di rete (di telecomunicazioni) garantisce la sicurezza in un insieme di dispositivi collegati l'uno con l'altro da appositi canali di comunicazione (link) tali da permettere lo scambio da un utente all'altro di risorse, informazioni e dati in grado di essere visualizzati e condivisi attraverso dispositivi di accesso.

68.4Sicurezza dei Sistemi

La sicurezza dei sistemi include tutte quelle misure di sicurezza volte a tutelare le informazioni tratte o gestite tramite elaboratori in modo da ridurre al minimo, i rischi:

1) di distruzione o perdita, anche accidentale delle stesse;
2) di accesso non autorizzato;
3) di effettuazione di operazioni non consentite.

68.5Sicurezza organizzativa

Le Misure di Sicurezza organizzativa integrano i controlli e le contromisure di Sicurezza Logica e Fisica tramite la definizione, l'adozione e gestione di modelli organizzativi comprendenti la separazione funzionale, aspetti di formazione, conformità, metodologie, audit e controllo, analisi vulnerabilità e minacce, ecc.

68.6Sicurezza Fisica

Le misure di sicurezza fisica sono volte a garantire il controllo degli accessi fisici onde impedire l'ingresso a persone non autorizzate che possono creare, volontariamente o no, danni o interferenze. Sono inoltre fondamentali per garantire un sufficiente grado di

protezione del patrimonio informatico da eventi di origine naturale o dolosa che possono in qualche misura minare l'integrità e la disponibilità dei sistemi e ovviamente dei dati. Il perimetro di interesse è esteso sia agli ambienti di lavoro sia agli ambienti tecnologici quali data center, nodi di rete, alle infrastrutture ed agli impianti.

68.7Disaster Recovery e continuità operativa

Le misure di Disaster Recovery e Continuità Operativa sono rispettivamente tutte quelle misure tecniche utili per affrontare un eventuale disastro che colpisce i sistemi informativi aziendali (es. catastrofi naturali come alluvioni o terremoti, errori umani, furti o attacchi hacker, ecc.) e l'insieme di attività volte a minimizzare gli effetti distruttivi, o comunque dannosi, di un evento che ha colpito un'organizzazione o parte di essa, garantendo la continuità delle attività più in generale.

69 Sicurezza delle Identità

E' di fondamentale importanza la possibilità di identificare e riconoscere le persone che utilizzano e trattano i dati, fra cui in modo particolare i dati personali. La responsabilità individuale nei trattamenti è fondamentale per poter prevenire e correggere comportamenti che, sia per errore che per volontà, possano minare l'integrità, la disponibilità e la riservatezza dei dati.
La creazione di un sistema in grado di gestire correttamente l'abbinamento fra l'identità dei soggetti e le attività che gli stessi svolgono nell'ambito delle informazioni non solo è da deterrente per ogni attività dolosa ma contribuisce a creare ed elevare la consapevolezza e responsabilità, che è alla base della sicurezza delle informazioni e del principio di Accountability espresso dal regolamento europeo.
La mancanza di un solido impianto per la sicurezza delle identità impedisce una corretta applicazione del modello organizzativo e delle autorizzazioni e deleghe ad operare sul dato personale.

69.1Principali caratteristiche di un sistema di sicurezza delle identità

Di seguito un elenco non esaustivo delle principali caratteristiche di cui deve disporre un sistema di sicurezza delle identità:

1) Ogni soggetto (interno o esterno) che possa avere accesso a qualsiasi informazione classificata (ad esclusione quindi delle informazioni definite pubbliche) deve essere identificato registrando la sua identità in un apposito archivio.
2) L'identità del soggetto deve essere univoca e verificata o attraverso un documento di identità valido o attraverso il riconoscimento per mezzo di sistema pubblico di identità digitale (CNS/SPID).

3) Le identità digitali devono essere manutenute correttamente nel tempo attraverso un idoneo ciclo di vita.
4) Tutte le credenziali di accesso (digitali o fisiche) alle informazioni devono essere sempre nominali e associate ad una identità certa.
5) Le credenziali di accesso devono essere basate su una logica di profilazione degli utenti in base alla organizzazione aziendale e al ruolo ricoperto dall'utente rispettando comunque il principio del minimo privilegio.
6) Nella progettazione dei profili degli utenti o durante il processo di richiesta di credenziali discrezionali (ah hoc) è necessario prendere in esame gli aspetti di Segregation of duty (SOD) per evitare che un soggetto possa ricevere autorizzazioni applicative potenzialmente in conflitto fra di loro e/o che possano introdurre vulnerabilità nel sistema informativo. Il conflitto fra autorizzazioni può essere inteso sia in senso assoluto (autorizzazioni che non possono mai coesistere su uno stesso soggetto) sia in termini di utilizzo in contemporanea (autorizzazioni che possono essere assegnate e coesistere su un soggetto ma che non possono essere mai accessibili nello stesso istante)
7) Ogni accesso alle risorse informative e servizi dell'ente, di qualsiasi natura e tipologia, necessita di un'autorizzazione formale, fornita (salvo differenti disposizioni particolari) da un Responsabile della struttura organizzativa proprietaria delle informazioni o da un responsabile gerarchico in base ad un modello autorizzativo predefinito. Qualsiasi accesso a risorse informative o servizi aziendali che avvenga senza aver prima richiesto e ottenuto formale autorizzazione è da considerarsi una violazione della sicurezza.
8) Nel caso in cui si creino credenziali di accesso ai sistemi automatici (M2M) queste devono essere ricondotte comunque ad una identità di un soggetto in grado di gestirle e manutenerle nel tempo (es. sistemista, DBA, ecc.) che ne è responsabile.
9) L'accesso a funzioni privilegiate deve essere limitato agli utenti che ne hanno effettiva necessità. La gestione dei profili privilegiati deve rispondere ai seguenti principi:

a) devono essere identificati gli utenti o le categorie di utenti alle quali devono essere concessi i privilegi;
b) i privilegi devono essere concessi solo se esiste una reale necessità, caso per caso sulla base di specifiche esigenze.

10) Anche le credenziali utilizzate per attività di gestione e manutenzione dei sistemi e delle reti devono essere nominali e riconducibili ad una identità. Qualora questo non sia possibile per ragione tecniche insuperabili (es. sistemi di rete obsoleti) è necessario gestire comunque la tracciabilità fra l'utilizzo della credenziale generica (es. administrator) l'identità dell'utilizzatore e il periodo di utilizzo.
11) E' possibile che un soggetto possegga anche più credenziali per accedere alla medesima fonte informativa sempreché tutte le credenziali facciano capo in modo certo e univoco alla medesima identità.

12) Qualsiasi credenziale che non sia riconducibile ad una identità deve essere immediatamente disabilitata rendendo impossibile l'accesso a qualsiasi tipologia di informazione.
13) Non è possibile riassegnare ad altri credenziali già usate nel passato per soggetti diversi.
14) Le attività dei soggetti all'interno dei sistemi informativi devono essere tracciate compatibilmente con quanto previsto e richiesto dalla normativa vigente e dall'analisi dei rischi. Le attività devono essere ricondotte ad una credenziale di accesso e a sua volta alla identità digitale.
15) Le indicazioni si devono applicare anche per gli accessi fisici ai locali dell'Ente richiedendo sempre l'identificazione del soggetto accedente.
16) Nel caso in cui un soggetto non abbia più nessuna collaborazione con Regione Toscana e si renda necessario la sua dismissione e relativa chiusura di tutte le sue credenziali è necessario che la sua identità, le sue credenziali e i log delle attività rimangano memorizzate all'interno degli archivi per un tempo necessario a poter garantire la ricostruzione dell'operato del soggetto nel tempo. I tempi di conservazione devono essere comunque conformi alle normative vigenti fra cui in modo particolare il regolamento 679/16.
17) Tutte le identità e le credenziali devono essere verificate e ricontrollate da parte dei responsabili con cadenza periodica.

70 Sicurezza dei Dispositivi di Accesso

Per "dispositivi di accesso" si intendono tutti gli apparati hardware e virtuali che consentono la visualizzazione e la modifica di informazioni contenute all'interno dei sistemi attraverso l'utilizzo delle reti. I dispositivi di accesso possono essere dotati di sistemi di memorizzazione locale in grado di archiviare sia informazioni provenienti dai sistemi, sia informazioni create ed elaborate direttamente in locale.
Le misure di sicurezza per i dispositivi di accesso impediscono l'uso improprio, accidentale o doloso del dispositivo stesso in grado di generare una vulnerabilità all'interno dei sistemi.

70.1 Dispositivi Trusted vs UnTrusted

I dispositivi di accesso ai dati possono essere classificati in due grandi insiemi:

- Dispositivi TRUSTED
- Dispositivi UNTRUSTED

Un dispositivo può essere definito "Trusted" quando è gestito in modo tale da ridurre al minimo i rischi di Sicurezza sui dati legati al suo utilizzo, a causa di errori, dolo o per omissione sia da parte dell'utilizzatore sia di azioni automatizzate (es. dispositivi messi a disposizione e gestiti da parte di Regione Toscana)

Qualsiasi altro dispositivo che non rientra nella categoria dei “TRUSTED” è da considerarsi, di conseguenza, “Untrusted” e, come tale, deve accedere ai dati attraverso modalità tecniche che garantiscano comunque un livello di sicurezza non minore di quelle dei dispositivi “Trusted” (in questa categoria rientrano ad esempio i dispositivi di proprietà dei dipendenti, collaboratori e consulenti esterni).

70.2 Principali caratteristiche per la sicurezza dei dispositivi di accesso

Di seguito un elenco non esaustivo delle principali caratteristiche di cui deve disporre un sistema di sicurezza dei dispositivi di accesso:

1) Ogni tipologia di dispositivo può accedere o meno ad una categoria di informazione in base alla sua classificazione di riservatezza. L’abbinamento fra la tipologia di dispositivo e la classe di informazione deve essere definita in appositi documenti di dettaglio.
2) Per ogni tipologia di dispositivo potranno essere definite regole di accesso in base alla sua classificazione a rete/sistemi. L’abbinamento fra la tipologia di dispositivo e la rete/sistema deve essere definita in appositi documenti di dettaglio.
3) La possibilità di copiare dei dati dalla rete/sistemi verso un dispositivo di accesso nella sua memoria in locale o al contrario di trasferire dai dati prodotti in locale in un dispositivo verso la rete/sistema deve essere definita ed espressamente autorizzata da appositi documenti di dettaglio.
4) I dati non possono mai risiedere in via esclusiva sui dispositivi di accesso (a prescindere dalla loro classificazione). Il dato master deve risiedere sempre all’interno dei dischi di rete dell’azienda.
5) Devono essere predisposti dei meccanismi automatici di sincronizzazione del dato in locale verso i dischi di rete aziendale al fine di salvaguardare l’integrità e la disponibilità del dato. La copia del dato da locale ai dischi di rete non deve essere lasciata alla mera volontà degli utenti.
6) I dispositivi “Untrusted” non possono, di norma, memorizzare dati in locale provenienti dalla rete/sistemi; eventuali dati memorizzati devono essere cancellati al termine del loro utilizzo
7) L’utilizzo di dispositivi UNTRUSTED all’interno di reti e sistemi di Regione Toscana deve essere espressamente autorizzato
8) I dispositivi “Untrusted” non possono copiare informazioni prodotte in locale all’interno dei dischi di rete/sistemi.
9) Deve essere garantita, con soluzioni allo stato dell’arte, la riservatezza dei dati da chi non sia in possesso delle credenziali, anche a fronte di azioni dolose (es. cifratura dei dischi).

10) Ogni dispositivo aziendale deve essere censito ed assegnato univocamente ad un soggetto utilizzatore o gestore che garantisce il rispetto di tutte le policy di sicurezza e ne è responsabile.
11) I dispositivi non ancora assegnati (magazzino, spare, jolly, ecc) devono essere custoditi in modo da impedire il loro utilizzo.
12) Devono essere emesse policy di utilizzo del dispositivo che garantiscano la continuità operativa e la salvaguardia dei dati in esso eventualmente memorizzati.
13) In caso di restituzione o dismissione di un dispositivo o di un supporto di memoria rimovibile si deve provvedere alla cancellazione in modo sicuro delle informazioni sugli stessi contenute, incluse le eventuali aree-disco temporanee del dispositivo utilizzate per la memorizzazione delle informazioni durante la sessione di lavoro. Il procedimento di rimozione deve avvenire in modo che le informazioni non siano più recuperabili.
14) Compatibilmente con i vincoli tecnologici e di budget è necessario definire degli standard relativamente ai dispositivi hardware, software e alle configurazioni da utilizzarsi al fine di aumentare il livello di sicurezza sia attraverso un maggior controllo delle vulnerabilità (minori variabili in gioco) sia attraverso una maggior intercambiabilità e sostituibilità dei dispositivi in grado di aumentare il livello di continuità operativa.

71 Sicurezza delle Reti

Le reti, attraverso i dispositivi di accesso, consentono agli utilizzatori (fra cui anche gli stessi elaboratori) di poter accedere al patrimonio informativo.
Le misure di sicurezza delle reti sono attuate adottando misure volte a proteggerne la riservatezza, l'integrità e disponibilità delle informazioni in transito attraverso la stessa rete.
Le principali misure nell'ambito delle misure di Sicurezza per la rete riguardano i seguenti ambiti:

1) ***Segregazione tra ambienti di rete***
2) ***Continuità del servizio***
3) ***Controllo degli accessi alla rete e ai sistemi***
4) ***Definizione di contesti classificati per operatività.***

71.1 Principali caratteristiche per la sicurezza delle Reti

Di seguito un elenco non esaustivo delle principali caratteristiche di cui deve disporre un sistema di sicurezza delle Reti:

1) Le reti devono essere in linea di principio segregate attraverso la creazione ambienti isolati tra loro o separati esclusivamente da un hardware o software con funzionalità di "firewall" che ne regolamenta le eventuali comunicazioni. La segregazione deve evitare il propagarsi di traffico indesiderato o malevolo tra i diversi utenti e tra gli utenti e le reti differenti garantendo il più possibile i principi di riservatezza e disponibilità delle informazioni.
2) La progettazione delle misure di sicurezza per ottenere la segregazione dei diversi Ambienti deve essere eseguita e commisurata con riferimento agli impatti che la mancanza di regole avrebbe sull'esercizio della rete nella sua globalità
3) Il collegamento di dispositivi a reti che consentono di accedere direttamente a risorse di rete privilegiate (es. applicativi interni, share di rete, ecc.) deve avvenire sempre attraverso un'Autenticazione dell'utente alla rete stessa attraverso l'uso di credenziali autorizzate.
4) Tutti i dispositivi che accedono alla rete Intranet aziendale dovranno essere profilati identificando a quali risorse e servizi possono accedere in una logica di minimo privilegio.
5) L'accesso fisico ai dispositivi di rete (cablati o wireless) deve essere coerente sia con logiche di segregazione dei segmenti di rete (in base ai servizi accedibili) sia con le logiche di segregazione imposte dalle politiche di sicurezza fisica.
6) Deve essere presente un sistema di gestione delle patch che consenta la gestione e distribuzione, preferibilmente centralizzata, degli aggiornamenti del software degli apparati.
7) Deve essere implementato un sistema di backup delle configurazioni che consenta di garantire l'accesso o il ripristino delle configurazioni in tempi brevi.
8) Deve essere implementato un sistema di monitoraggio che consenta la visualizzazione, memorizzazione ed analisi delle performance degli apparati.
9) Deve essere presente un sistema di gestione dei log quale punto di raccolta centralizzato dei log provenienti dagli apparati

72 Sicurezza dei Sistemi

Le politiche di sicurezza dei Sistemi includono tutte quelle misure di sicurezza volte a garantire la Riservatezza, l'Integrità e la Disponibilità delle informazioni aziendali elaborate e contenute all'interno delle architetture IT in modo da ridurre al minimo, i rischi di distruzione o perdita, anche accidentale delle stesse; di accesso non autorizzato; di effettuazione di operazioni non consentite.

72.1Principali caratteristiche per la sicurezza dei Sistemi

Di seguito un elenco non esaustivo delle principali caratteristiche di cui deve disporre un sistema di sicurezza dei sistemi:

1) In ogni sistema dovrebbe essere presente un sistema di "Log Management" quale punto di raccolta centralizzato dei log provenienti dai dispostivi presenti nell'infrastruttura IT; tra questi i più diffusi sono gli eventi di Sistema Operativo e DataBase, sistemi di sicurezza, network elements e servizi applicativi in genere. La memorizzazione dei log raccolti deve essere basata su di un sistema avanzato di controllo di integrità, per garantire che i log memorizzati non siano stati manomessi.

2) In ogni sistema dovrebbe essere presente un "Security Information and Event Management (SIEM)" in grado di completare le funzionalità di log collecting con quelle di analisi dei log in tempo reale per dare evidenza degli eventi critici di sicurezza nell'infrastruttura IT. Dovrebbero anche essere presenti le funzionalità di analisi dei dati storici e di reportistica sui log memorizzati.

3) Dovrebbe essere presente un sistema di "Discovery and Dependency Mapping" in grado di identificare e mappare le dipendenze dei server aziendali, delle applicazioni e dei dispositivi di rete. La soluzione deve garantire un'integrazione diretta e una sincronizzazione in tempo reale con la componente di Configuration Management Database (CMDB), assicurando che i dati presenti nel CMDB siano sempre aggiornati rispetto alle modifiche apportate.

4) Dovrebbe essere presente un sistema di "Performance, Availability, Event & Impact Management" in grado di semplificare le operazioni del personale IT gestendo e monitorando il funzionamento dell'infrastruttura IT, prevenendo i problemi, identificando automaticamente le possibili cause nei vari silos tecnologici e avviando processi di valutazione e risoluzione dei problemi standardizzati. Il sistema di Performance Management dovrebbe consentire di rilevare automaticamente le relazioni intercorrenti tra i servizi aziendali memorizzate dentro il CMDB al fine di svolgere un'analisi più accurata delle possibili cause con un minor impiego di persone per la valutazione dei problemi.

5) Dovrebbe essere presente un sistema di "Incident and Problem Management" in grado di offrire un insieme di soluzioni integrate (anche al CMDB ed al sistema di monitoring) ed orientate ai servizi che permette di gestire gli incidenti e i problemi con un approccio proattivo, automatico e uniforme, basato sulle best practice dello schema ITIL.

6) I sistemi dovrebbero essere protetti da un appropriato sistema di controllo degli accessi. Il livello di sicurezza richiesto dipende dalla criticità del sistema e delle informazioni in esso contenute e corrisponderà alle scelte effettuate dal Sistema di Gestione della sicurezza dell'informazione e seguirà le procedure emanate da parte del Comitato di sicurezza. Nel caso di accesso a sistemi particolarmente vulnerabili o critici dovranno essere identificati sistemi di autenticazione forte alternativi o complementari ai sistemi di accesso di base.

7) Deve essere presente un sistema di “Identity Access Management (IAM)” in grado di gestire in automatico il ciclo di vita degli utenti basato su policy nonché il controllo degli accessi per l'intero ente.
8) Dovrebbe essere implementato un sistema di “Backup Management” che consenta di garantire, in caso di guasti hardware o di problemi software, l'accesso o il ripristino dei dati aziendali in tempi brevi.
9) Dovrebbe essere implementato un sistema di “Antivirus Management” per la gestione della protezione antivirus della rete IT aziendale (server, desktop e file server)
10) Dovrebbe essere presente un sistema di “Patching Management” che consenta la gestione e distribuzione centralizzate degli aggiornamenti del software, e che automatizza la rilevazione delle vulnerabilità della sicurezza facilitandone il rimedio:
11) Dovrebbe essere presente un sistema di Hardening Management per l’attivazione di un processo di verifica e messa in sicurezza degli host, mediante l’adozione di specifiche tecniche per ridurre i punti di attacco da parte di un hacker.
12) Dovrebbero essere presenti dei servizi di “Reverse Proxy Management” che si occupino di effettuare uno "store and forward" del traffico diretto verso una delle risorse gestite (unico punto di transito e controllo delle chiamate alle varie applicazioni poste in zona demilitarizzata).
13) Dovrebbe essere implementato il protocollo Network Time Protocol (NTP) per consentire di sincronizzare l’orologio interno di un sistema attraverso uno o più time server, rendendo così la data del sistema affidabile e conseguentemente anche quella ridistribuita ai client della rete locale.
14) Dovrebbe essere implementato un sistema di Firewall Management che consenta di proteggere il perimetro della rete IT aziendale dagli attacchi più comuni definendo opportune Access Control List e Policy.
15) Dovrebbe essere implementato un sistema di Vulnerability scanning / assessment in grado di analizzare l'eventuale presenza di vulnerabilità per i sistemi ed i servizi esposti, con identificazione delle possibili ed ulteriori contromisure da attivare.

73 Sicurezza Organizzativa

Obiettivo di tali politiche è quello di integrare i controlli e le contromisure di Sicurezza Logica e Fisica tramite la definizione e la gestione di raccomandazioni organizzative.

73.1 Principali caratteristiche per la Sicurezza Organizzativa

Di seguito un elenco non esaustivo delle principali caratteristiche di cui deve disporre un sistema di sicurezza d:

1) Conformità alle leggi in vigore. Per garantire tale principio le fonti normative devono costantemente essere monitorate;
2) Conformità alle normative emanate da Regione Toscana. Per garantire tale requisito deve essere costantemente monitorata l'emissione di Linea Guida e Normative da parte delle strutture dedicate alla gestione della Sicurezza e delle normative di Regione Toscana;
3) Continuo aggiornamento del Corpo Procedurale in base allo scenario tecnologico, agli incidenti di Sicurezza e alle attività di Auditing e Risk Assessment;
4) Allineamento dei processi di software management alle norme di legge che tutelano il diritto di proprietà intellettuale;
5) Censimento periodico delle informazioni e dei relativi processi e adozione di un sistema di classificazione delle informazioni in grado di suddividere le informazioni Aziendali in relazione al loro livello di riservatezza;
6) Analisi delle minacce attraverso lo studio di tutti gli agenti (esterni o interni) che possono causare un danno (impatto) sugli Asset di Regione Toscana;
7) Analisi delle vulnerabilità attraverso lo studio dei fattori di debolezza sia interni agli Asset (ovvero dipendenti dalle caratteristiche dell'Asset stesso) che esterni (ovvero dipendenti da carenze nella implementazione delle contromisure poste a protezione dell'Asset);
8) Calcolo periodico del valore del rischio considerando il valore dell'Asset, le vulnerabilità ad esso associate, le minacce a cui è sottoposto e la loro probabilità di accadimento;
9) Individuazione delle contromisure e dei controlli da implementare sulla base del livello di rischio calcolato e di una analisi dei costi/benefici (derivanti dalla implementazione dei controlli e delle contromisure di sicurezza);
10) Pianificazione ed esecuzione periodica dei controlli di sicurezza al fine di monitorare la corretta applicazione delle Politiche Regionali, le normative e le procedure di sicurezza in essere. Revisione delle politiche e del sistema di gestione della sicurezza delle informazioni anche in base agli esiti dei controlli.
11) Definizione di obiettivi per la sicurezza delle informazioni che:
    a) siano coerenti con le politiche emesse
    b) siano misurabili
    c) tengano conto degli elementi emersi dall'analisi dei rischi,
    d) siano comunicati alla struttura
    e) siano aggiornati
12) Formazione di tutto il personale destinato a gestire informazioni aziendali sulla rilevanza strategica di un Sistema di Gestione della sicurezza delle Informazioni;
13) Definizione di accordi di riservatezza e non divulgazione previsti dal contratto di lavoro, dal Codice Etico e dalle disposizioni aziendali sulla privacy per i dipendenti

che ricoprono incarichi strategici e/o che hanno necessità di accedere a informazioni aziendali;

14) Informazione ed istruzione di tutto il personale sugli aspetti di sicurezza e sul Corpo Procedurale di Sicurezza attraverso la diffusione di un preciso e definito programma di sensibilizzazione. L'efficacia di tali programmi deve essere verificata periodicamente;

15) Gestione della continuità operativa comprendente tutte le iniziative volte a ridurre a un livello ritenuto accettabile i danni conseguenti a incidenti/catastrofi che colpiscono direttamente o indirettamente l'Azienda;

16) Gestione degli incidenti con particolare attenzione alla definizione di processi e procedure operative per il governo dell'emergenza ed il ripristino della continuità operativa. Definizione dei processi e regole per la segnalazione e registrazione degli incidenti agli organismi interni e ad eventuali organismi esterni quando richiesto dalla legge (es. segnalazioni al garante privacy)

17) Definizione di normative comportamentali volte a regolamentare aspetti quali: Principi generali di comportamento e di controllo, utilizzo delle postazioni di lavoro, Back-up e utilizzo dei supporti magnetici, Eventi lesivi e modalità di segnalazione, Identificazione e autenticazione degli utenti, Utilizzo delle risorse di rete, Utilizzo della Posta Elettronica, Utilizzo di Internet, Clean Desk e Clean Screen Policy, Segnalazione degli incidenti di sicurezza logica, ecc

18) Tutto il Sistema di Gestione della Sicurezza delle Informazioni (SGSI) deve essere strutturato sulla base di un classico modello PDCA

74 Sicurezza Fisica

La Sicurezza Fisica definisce e regolamenta le modalità di protezione dei beni fisici Regionali (persone, strutture, macchinari, documentazione).

1) Al fine di garantire il controllo degli accessi dei Dipendenti, Fornitori e utenti di Regione Toscana e per la sicurezza fisica nel Data Center devono essere identificati diversi livelli di accesso.

2) I livelli di accesso fisico devono essere coerenti con:
   a) ruolo e responsabilità delle varie tipologie di utenti ammessi.
   b) accesso alle risorse di rete e sistemi

3) Gli accessi fisici vanno controllati attraverso sistemi di autorizzazione e monitoraggio degli accessi alle sedi, accessi alle sale macchine del Data Center, sistemi anti-intrusione, ecc.

4) Ogni soggetto (interno o esterno) che possa avere accesso ai locali di Regione Toscana deve essere identificato registrando la sua identità in apposito archivio. L'identità del soggetto deve essere verificata o attraverso un documento di identità valido.

5) Ogni accesso ai locali di Regione Toscana necessita di un'autorizzazione formale, fornita (salvo differenti disposizioni particolari) da un Responsabile in base ad un

modello autorizzativo predefinito. Qualsiasi accesso ai locali di Regione Toscana senza aver prima richiesto e ottenuto formale autorizzazione è da considerarsi una violazione della sicurezza.

6) Il rilascio delle credenziali di accesso (es. badge, chiavi meccaniche, ecc.) deve essere basato su una logica di profilazione degli utenti in base alla organizzazione aziendale e al ruolo ricoperto dall'utente rispettando comunque il principio del minimo privilegio.
7) E' necessario mantenere la registrazione di tutti gli accessi effettuati alle aree protette (es. Data Center) associati univocamente alle credenziali (es. badge) utilizzati per l'accesso.
8) Deve essere gestito e manutenuto un inventario di tutti gli apparati installati presso i locali di Regione Toscana con una particolare attenzione ai locali protetti (es. Data Center). L'inventario deve essere costantemente aggiornato sia per le nuove installazioni sia per le sostituzioni o rimozioni di componenti. Ogni ingresso o uscita di apparecchiature Hardware dai locali protetti (es. Datacenter) deve essere controllato ed espressamente autorizzato.
9) La Sicurezza ambientale va gestita attraverso l'adozione di Sistemi antincendio, Allarmi antiallagamento, continuità dell'alimentazione elettrica, allarmi ambientali, ecc.
10) I locali destinati ad archivi per le copie di sicurezza dei dati vanno protetti attraverso sistemi di serrature a chiave non duplicabile, armadi e casseforti di sicurezza e ignifughe, ecc.
11) i documenti e i supporti contenenti dati sensibili o giudiziari devono essere custoditi in appositi archivi ad essi esclusivamente dedicati;
12) Tutti i dati personali non più necessari, fatto salvo i casi prescritti dalla legge, devono essere distrutti e rimossi dagli archivi.
13) aree a cui si applicano i controlli descritti nella presente linea guida, sono definite "aree protette". In particolare, le "aree protette" sono tutte quelle aree che possiedono almeno una di queste caratteristiche:
    a. aree in cui sono presenti le postazioni operative per la gestione e monitoraggio del Datacenter e della rete;
    b. aree in cui sono presenti postazioni dedicate allo sviluppo e test;
    c. aree in cui sono presenti apparecchiature critiche di rete, del Datacenter e di supporto.

Le misure che si adottano per controllare l'accesso a tali "aree protette" sono tese a garantire un adeguato livello di sicurezza, che consenta l'ingresso e la permanenza nei locali esclusivamente del personale in turno di servizio o di personale autorizzato, prevenendo furti e danneggiamenti alle apparecchiature o accesso non autorizzato alle informazioni.
I controlli applicati per le diverse aree descritte nelle presenti politiche possono differire in funzione della tipologia delle risorse del Sistema Informativo che vi sono allocate.

75 Disaster Recovery e Continuità Operativa

Le misure di Disaster Recovery indicano tutte le misure tecniche utili per affrontare un eventuale disastro che colpisca i sistemi informativi aziendali e che può avere diversa origine: catastrofi naturali come alluvioni o terremoti, errori umani, furti o attacchi hacker. Il piano di Disaster Recovery stabilisce in primis quali sono i processi aziendali critici per un business, ossia quelli che devono essere maggiormente monitorati e protetti. Definisce poi i parametri di RTO e RPO (tempi di ripristino e livello di perdita dati accettabile) a seconda delle esigenze della specifica azienda e pianifica le azioni da intraprendere per il ripristino totale e più rapido possibile di sistemi, dati e applicazioni in caso di incidente.
Le misure di Business Continuity, invece, si riferiscono ad una soluzione globale, che comprende tutte le procedure e i processi che hanno lo scopo di garantire la continuità del business e di evitare l'interruzione delle attività, sia dovute a disservizi del reparto IT che a cause di altra natura, come ad esempio incidenti di origine legale, o fermo dell'attività causato da mancanza di personale. La strategia di Business Continuity tiene conto di tutti gli eventi che possono minacciare la sopravvivenza del business ed è utile anche nel caso di interruzioni minori dell'operatività.
In linea di massima, quindi, le misure di Disaster Recovery e Business Continuity sono misure di sicurezza fondamentali per garantire la disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali, e nel contempo garantire la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico come richiesto dall'art. 32 del GDPR.

75.1 Principali caratteristiche per la Business Continuity e Disaster Recovery

1) E' necessario determinare i propri requisiti per la sicurezza delle informazioni e per la continuità della gestione della sicurezza delle informazioni in situazioni avverse, per esempio durante crisi o disastri, individuando i processi per la gestione tempestiva di possibili eventi critici futuri che potrebbero minacciare la sopravvivenza dell'ente.
2) Occorre stabilire, documentare, attuare e mantenere processi, procedure e controlli per assicurare il livello di continuità richiesto per la sicurezza delle informazioni durante una situazione avversa.
3) Occorre verificare ad intervalli di tempo regolari i controlli di continuità della sicurezza delle informazioni stabiliti e attuati, al fine di assicurare che siano validi ed efficaci durante situazioni avverse.
4) Le strutture per l'elaborazione delle informazioni devono essere realizzate con una ridondanza sufficiente a soddisfare i requisiti di disponibilità prevedendo se necessario anche soluzioni di Disaster Recovery.

76 Misure di sicurezza “specifiche” per la Data Protection

Nonostante il sistema di misure di sicurezza contenuto nel GDPR non preveda più un elenco tassativo e specifico di misure minime (come nel Codice Privacy – Dlgs 196/03), in diversi passaggi, primo fra tutti l’art. 32 comma 1 (oltre al considerando nr. 83), si indicano la cifratura dei dati e degli archivi e la pseudonimizzazione delle informazioni, come tecniche suggerite per aumentare la protezione dei dati, soprattutto di quelli di particolari categorie (es. dati giudiziari, dati sanitari, religiosi, ecc.).
L’idea è quella che un’eventuale fuga di questi dati faccia sì che le informazioni reperibili siano visibili, ma assolutamente incomprensibili o destrutturate, ossia separate da altre informazioni che sarebbero in grado di dar loro un senso.
La crittografia e pseudonimizzazione richiedono comunque la definizione di precise regole (“policy”) per una corretta gestione del sistema e per normare anche i comportamenti degli utenti che altrimenti rischierebbero di inficiare l’efficacia di questi due strumenti di sicurezza.
Si tratta quindi di meccanismi che di certo riducono i rischi connessi al trattamento di dati personali e che contribuiscono a rendere i titolari/responsabili del trattamento conformi alle nuove regole sulla privacy aumentando notevolmente il livello di riservatezza, ma che a volte rendono più onerosa la gestione del dato e, in taluni casi, possono introdurre anche potenziali vulnerabilità in ambito disponibilità e integrità dell’informazione.
L’uso quindi di tali tecniche non deve essere indiscriminato e condotto a tappeto su tutti i dati e trattamenti, ma deve essere sempre ricondotto ad una valutazione di rischio/opportunità, nella quale rimangono centrali sia i diritti dell’interessato sia le capacità organizzative e di spesa dell’ente.

76.1 Crittografia

La crittografia (o cifratura) si basa, di solito, su un algoritmo di cifratura e su una passphrase e/o token che “aprono” e “chiudono” i dati (di solito al momento dell’autenticazione). Si tratta di una procedura che è trasparente per l’utente ma che protegge l’informazione con modalità che sono, nella maggior parte dei casi, indecifrabili.
La cifratura può diventare uno strumento di protezione fondamentale per grandi quantità di dati, per sistemi che gestiscono credenziali, per quelli che trattano dati sensibili (dati sanitari, giudiziari, ecc.), per i computer che processano una grande mole d’informazioni per profilare i consumatori. Peraltro, l’utilizzo della cifratura offre un’ulteriore tutela anche nei confronti del titolare/responsabile che nel caso di data breach (accertato) è molto probabilmente esentato dall’obbligo di comunicare l’evento alle autorità di controllo e agli interessati in considerazione del fatto che è molto improbabile che la violazione dei dati personali (cifrati) presenti un rischio per i diritti e le libertà delle persone fisiche.

76.2 Pseudonimizzazione

L’uso di pseudonimi prevede il trattamento dei dati personali in modo tale che essi non possano più essere attribuiti ad un interessato specifico senza l’utilizzo di informazioni

aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative tese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.
Può essere usato, ad esempio, un unico pseudonimo riferito ad un insieme univoco di dati, ma anche un singolo pseudonimo per ogni specifico dato.
In sostanza, la pseudonimizzazione perché sia efficace, deve:

a. prevedere l'assenza di identificabilità diretta del soggetto interessato (trattamento dei dati personali in modo tale che i dati non possano essere più attribuiti ad un interessato specifico senza l'utilizzo di informazioni aggiuntive);
b. adottare misure di sicurezza ulteriori da aggiungere alla pseudonimizzazione;
c. incorporare la pseudonimizzazione nella privacy-by-design (misure tecniche e organizzative volte a garantire che tali dati personali non siano più attribuibili ad una persona fisica).

E' importante sottolineare che, se da una parte l'utilizzo delle tecniche di pseudonimizzazione, oltre che essere richiamato e caldeggiato in vari punti del regolamento europeo, rappresenta una delle tecniche più importanti ed interessanti ai fini della protezione del dato personale, dall'altra spesso non garantisce in modo assoluto, (da sola) la protezione del dato personale.
Rimane, infatti, fondamentale accertarsi che i dati, resi privi, della loro identificabilità diretta (processo di pseudonimizzazione) non consentano comunque, attraverso la loro interpretazione e correlazione, di ricondurre comunque ad un soggetto univoco.

76.3 Anonimizzazione

Mediante l'anonimizzazione, viene rimosso e/o modificato qualsiasi elemento riconoscibile che possa consentire di risalire ad un soggetto specifico identificandolo sia attraverso dati anagrafici/identificativi diretti (es. nome, cognome, codice fiscale, ecc.), sia attraverso la correlazione di informazioni "secondarie" che, opportunamente associate ed elaborate, possono comunque portare all'identificazione del soggetto (altezza, peso, data di nascita, ecc.)
A questo punto il dato perde il suo status di dato personale (pur mantenendo comunque una valenza statistica/business) rendendo quindi non necessarie particolari forme di protezione dello stesso.
Le tecniche di anonimizzazione possono essere molteplici; si citano, ad esempio, le seguenti:

- Aggiunta del rumore statistico -> tecnica che consiste nell'alterazione degli attributi contenuti in un set di dati in modo tale da renderli meno precisi, mantenendo allo stesso tempo la composizione generale (es. arrotondamento di alcuni valori).
- Generalizzazione -> tecnica che consiste nell'estendere le scale di grandezza, generalizzando gli attributi riferiti ad uno stesso gruppo di soggetti (ad es. un mese al posto di una settimana; una regione al posto di un paese).

- Scrambling -> tecnica che consente di offuscare le lettere dell'alfabeto mescolandole tra loro o sostituendole con simboli e/o lettere speciali.

Nei processi di anonimizzazione (per loro natura irreversibili) si tenga presente che i diritti dell'interessato non sono limitati alla sola riservatezza ma spesso anche ai principi di disponibilità ed integrità. Ciò significa che in taluni casi forme di anonimizzazione su alcuni trattamenti potrebbero garantire la riservatezza, ma nel contempo potrebbero ledere i diritti dell'interessato non consentendo più allo stesso di esercitare i propri diritti (es. accesso e portabilità del dato)

77 Coclusioni

Le presenti linee guida hanno lo scopo di fornire oltre che una riflessione complessiva sul SGSI in merito ai livelli di sicurezza disponibili e attuati, una guida per la verifica periodica dei livelli di sicurezza andando a specificare per ogni voce riportata in queste linee guida, cosa sia disponibile, i livelli di miglioramento e il piano della loro attuazione in modo da avere sempre una fotografia aggiornata della situazione.
Occorre sempre bilanciare :

1) le minacce intese come eventi che hanno una certa probabilità di avverarsi e una loro pericolosità (magnitudo),
2) i rischi susseguenti all'avverarsi delle minacce
3) Le misure o contromisure che possono essere messe in campo al fine di ridurre il rischio o il danno per l'interessato o categoria di interessati.

Questo rappresenta non una singola iniziativa, ma un lavoro, un processo continuo teso a creare la consapevolezza del livello di sicurezza o meno del proprio sistema informativo e a valutarne il livello di adeguatezza

Allegato C

Clausole Contrattuali Titolare – Titolare
(Titolari Autonomi)

1 Scopo del documento

Il presente documento ha per obiettivo quello di fornire un facsimile di accordo Data Protection (Data Protection Agreement) nel caso in cui la relazione che si viene ad istaurare per il trattamento di dati personali sia fra due soggetti che a norma del GDPR si possano classificare come Titolari autonomi rispetto ai trattamenti nei quali vengono coinvolti dati personali.
Si tratta di due o più soggetti giuridicamente diversi che hanno la piena titolarità dei trattamenti in quanto attivati sulla base di specifiche norme e finalità che ne determinano sia la titolarità che la liceità. Questi soggetti Titolari ognuno per le proprie finalità condividono o si trasferiscono dati personali e pertanto devono sottoscrivere un accordo, nel quale si da atto del riconoscimento reciproco della titolarità nell'eseguire quei trattamenti, dei dati condivisi o trasmessi, delle misure adottate a garantire un canale sicuro alle comunicazioni, ecc.
Il fac simile che segue, deve essere ovviamente compilato e personalizzato sulla base di quanto e come è oggetto di scambio informativo, pertanto costituisce una linea guida nella formalizzazione dell'accordo.
L'articolato che segue può essere oggetto di uno specifico accordo od essere inserito all'interno di atti convenzionali o protocolli di intesa che vengono sottoscritti per regolare anche altri rapporti oltre alla Data Protection.

78 Facsimile di Data Protection Agreement

Accordo Data Protection fra Titolari Autonomi
(Data Protection Agreement)

TRA

…… [specificare il nome del Titolare], con sede legale in …….. [specificare l'indirizzo della sede legale], in persona del suo legale rappresentante ……..[specificare il nome completo del legale rappresentante del primo Titolare] (

E

…… [specificare il nome dell'altro Titolare], con sede legale in …… [specificare l'indirizzo della sede legale dell'altro Titolare], in persona del suo legale rappresentante …… [specificare il nome complete del legale rappresentante dell'altro Titolare]

Titolare 1 e Titolare 2, verranno in seguito entrambi indicati come “la Parte” o congiuntamente “le Parti”.

Art. 1
Ambito di competenza

Le Parti si danno reciprocamente atto di conoscere ed applicare, nell’ambito delle proprie organizzazioni, tutte le norme vigenti ed in fase di emanazione in materia di trattamento dei dati personali, sia primarie che secondarie, rilevanti per la corretta gestione del Trattamento, ivi compreso il Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (di seguito “GDPR”).

Le parti si danno reciprocamente atto che lo scambio di dati oggetto del presente DPA risponde ai principi di liceità determinati da specifiche norme ed è conforme alle disposizioni.

Le parti si danno reciprocamente atto che lo scambio di dati oggetto del presente DPA è conforme alle disposizioni, alle linee guida e alle regole tecniche previste per l’accesso, la gestione e la sicurezza dei dati dalla normativa in materia di amministrazione digitale (in specifico, d.lgs. 82/2005 e relative linee guida e regole tecniche) e dalle altre norme di riferimento.

[

fare riferimento alle norme che supportano la liceità dei trattamenti derivanti dalla trasmissione/condivisione di dati personali oggetto del presente DPA e le finalità istituzionali perseguite

indicare le modalità con le quali si scambiano i dati (trasmissione, accesso e consultazione, interoperabilità e cooperazione applicativa, condivisione e fruizione in cloud...)

]

Art. 2
Rapporti fra autonomi Titolari di trattamento dati

Le Parti tratteranno in via autonoma i dati personali oggetto dello scambio per trasmissione o condivisione, per le finalità connesse all'esecuzione del *contratto/convenzione/protocollo di intesa* [*...inserire il riferimento ....]* (di seguito "Convenzione/contratto/protocollo di intesa"). Le parti, in relazione agli impieghi dei predetti dati nell'ambito della propria organizzazione, assumeranno, pertanto, la qualifica di Titolare autonomo del trattamento ai sensi dell'articolo 4, nr. 7) del GDPR, sia fra di loro che nei confronti dei soggetti cui i dati personali trattati sono riferiti.

Art. 3
Tipologia di dati oggetto di scambio

I contraenti in relazione allo scambio di informazioni, inteso sia come trasmissione di dati sia di condivisione di archivi e al loro ruolo di essere sorgente o destinatario delle informazioni scambiate si qualificano nel seguito come soggetto Produttore o soggetto Utilizzatore.

I dati personali oggetto dello scambio:

1. Soggetto produttore del dato: […….], soggetto utilizzatore: […….], Periodicità dello scambio di dati

    a. Tipologie di dati [*dati comuni, dati particolari, dati sanitari, dati giudiziari]*

    b. tipologie degli interessati *[numerosità, minori, disabili, ecc..]*

    c. I seguenti formati *[testo, immagini, file, cartacei, ecc..]*

2. Soggetto produttore del dato: […….], soggetto utilizzatore: […….], Periodicità dello scambio di dati: [……]

    a. Tipologie di dati [*dati comuni, dati particolari, dati sanitari, dati giudiziari]*

    b. tipologie degli interessati : *[numerosità, minori, disabili, ecc..]*
    c. I seguenti formati : [*testo, immagini, file, cartacei, ecc..]*

Nota: nel caso lo scambio sia bilaterale, altrimenti solo il primo.

Art.4
Rispetto della normativa

In quanto Titolari autonomi del trattamento, le parti sono tenute a rispettare tutte le normative rilevanti sulla protezione ed il trattamento dei dati personali che risultino applicabili ai rapporti che intercorrono fra produttore di informazioni e utilizzatore sulla base del presente DPA. Le Parti sono, altresì, tenute al rispetto della normativa in materia di amministrazione digitale e in materia di accesso, gestione e sicurezza dei dati.

Art. 5
Misure di sicurezza

Le parti concordano sull'adeguatezza delle misure di sicurezza messe in atto al fine di garantire lo scambio sicuro dei dati.
In particolare attestano la messa in atto delle seguenti misure:

[

elenco delle misure di sicurezza messe in atto nella trasmissione/condivisione delle informazioni

]

Al contempo, le parti, si impegnano a mettere in atto ulteriori misure qualora fossero da almeno una delle due parti ritenute insufficienti quelle in atto. L'eventuale diniego dell'altra parte comporta l'annullamento del presente DPA.
In particolare, l'utilizzatore si impegna ad applicare misure di sicurezza idonee e adeguate a proteggere i dati personali da esso trattati in esecuzione del presente Contratto e a rispettare i principi e le norme in materia di accesso, gestione e sicurezza dei dati, contro i rischi di distruzione, perdita, anche accidentale, di accesso o modifica non autorizzata dei dati o di trattamento non consentito o non conforme alle finalità della raccolta.

Art. 6
Obblighi del personale autorizzato

Le parti si impegnano a far sì che l'accesso ai dati personali oggetto dello scambio sia consentito solo a coloro e nella misura in cui ciò sia necessario per l'esecuzione del contratto/Convenzione/protocollo di intesa, e che l'uso dei dati personali da parte del soggetto utilizzatore rispetti gli stessi impegni assunti dal produttore riguardo alla conformità legale del trattamento e la sicurezza dei dati trattati con misure adeguate alla tipologia dei dati degli interessati e dei rischi connessi.
Ognuna delle parti individua un proprio referente tecnico, responsabile dell'accesso, della gestione e della sicurezza dei dati e dell'applicazione delle relative norme, linee guida e regole tecniche, tenuto a comunicare tempestivamente all'altra parte modifiche,

aggiornamenti, esigenze, problematiche, incidenti e quanto ritenuto necessario nella corretta gestione dei dati, al fine di assicurarne la conformità ai principi e alle disposizioni normative di riferimento.

Art.7
Responsabilità

Fatto salvo quanto previsto come inderogabile dalla legge, nessuna responsabilità sarà imputabile al produttore del dato per i trattamenti operati dall'utilizzatore (vedi art. 3), eccettuati i casi di cattiva gestione o maltrattamento nella fase di raccolta originaria dei dati personali. Ferma restando la responsabilità assunta dal produttore verso i terzi e verso l'utilizzatore, quale titolare autonomo del trattamento sui dati ricevuti dal produttore, nei rapporti reciproci, l'utilizzatore si obbliga a manlevare e tenere indenne il produttore – per qualsiasi danno, incluse spese legali – che possa derivare da pretese avanzate nei confronti del produttore da terzi - inclusi i soggetti cui i dati personali trattati sono riferiti - a seguito dell'eventuale illiceità o non correttezza delle operazioni di trattamento imputabili al utilizzatore, intendendosi con la presente pattuizione, trasferire dal produttore al utilizzatore l'incidenza economica dei danni reclamati da terzi, in conseguenza dei trattamenti operati dal utilizzatore.

Art. 8
Impostazione organizzativa

Le parti si garantiscono reciprocamente che i dati trattati da ciascuna di esse in esecuzione del presente DPA formano oggetto di puntuale verifica di conformità alla disciplina rilevante in materia di trattamento di dati personali - ivi compreso il GDPR-, alla normativa in materia di amministrazione digitale e in materia di accesso, gestione e sicurezza dei dati e si impegnano altresì alla ottimale cooperazione reciproca nel caso in cui una di esse risulti destinataria di istanze per l'esercizio dei diritti degli interessati previsti dall'articolo 12 e ss. del GDPR ovvero di richieste delle Autorità di controllo che riguardino ambiti di trattamento di competenza dell'altra parte.

Art. 10
Durata

Il presente Data Protection Agreement ha durata [……] dalla sua sottoscrizione

Art. 11
Rescissione

La rescissione del presente DPA avviene per istanza di parte qualora, la stessa ritenga che lo scambio di informazioni leda per qualsivoglia motivo i legittimi diritti degli interessati

Data --/--/----
Firma
Firma

Allegato D/E

Clausole Contrattuali Titolare – Responsabile

Data Protection Agreement

1 Scopo del Documento

Il presente documento costituisce la formulazione, aggiornata ai sensi del Reg. UE 2016/679, di un facsimile di accordo da stipulare fra Titolare e Responsabile nell'ambito di contratti o convenzioni. Tale regolazione del rapporto, può essere inserito all'interno dell'articolato dei contratti o convenzione o essere oggetto di un atto separato sottoscritto dalle parti.

Nel caso si configuri un rapporto con un terzo soggetto in qualità di sub responsabile andranno inserite le relative parti.

L'articolato può far parte di un accordo autonomo o inserito all'interno di contratti e convenzioni che regolano anche altri aspetti dei soggetti.

Il presente accordo può essere semplificato in considerazione della quantità, qualità e tipologia dei dati oggetto dei trattamenti che il Titolare demanda alla elaborazione da parte del Responsabile.

Definizioni:

Titolare il soggetto titolare delle finalità dei trattamenti e dei dati personali oggetto delle attività disciplinate dal contratto/convenzione

Responsabile il soggetto che effettua trattamenti di dati personali per conto del Titolare

Interessato la persona fisica cui si riferiscono i dati personali trattati

DPO Responsabile trattamento dati personali/Data Protection Officer

GDPR Regolamento Europeo sulla protezione dei dati personali 679/2016 – General Data Protection Regulation

Security IT Manager la persona o la struttura a cui sono demandate le attività di auditing sulle misure di sicurezza adottate e di incident management

Incident management procedura di gestione degli incidenti IT relativi a dati personali

Responsabile della sicurezza IT la persona o la struttura cui è demandato il compito di definire, impostare e gestire le misure di sicurezza IT

Lock-In con tale termine si intende la diminuzione o perdita da parte del titolare della possibilità di gestire i servizi e relativi dati in autonomia senza dover forzatamente ricorrere al soggetto a cui ne ha ceduto la gestione. La sicurezza dei dati e la continuità del servizio devono sempre essere sotto il controllo del Titolare.

79 Fac-simile di accordo

Accordo Data Protection fra Titolare, Responsabile (- sub Responsabile)
(Data Protection Agreement)

TRA

…… [specificare il nome del Titolare], con sede legale in …….. [specificare l'indirizzo della sede legale], in persona del suo legale rappresentante ……..[specificare il nome completo del legale rappresentante] (

E

…… [specificare il nome del Responsabile], con sede legale in …… [specificare l'indirizzo della sede legale del Responsabile], in persona del suo legale rappresentante …… [specificare il nome completo del legale rappresentante del Responsabile]

Titolare e Responsabile verranno in seguito entrambi indicati congiuntamente "le Parti".

ART. 1 TRATTAMENTO DEI DATI PERSONALI

Ai sensi e per gli effetti della normativa in materia di protezione dei dati personali (Reg. UE n. 2016/679, di seguito "GDPR", nonché D. Lgs. 196/2003 da ultimo novellato dal D. Lgs. 101/2018, di seguito "Codice Privacy") ed in relazione alle operazioni che vengono eseguite per lo svolgimento delle attività previste dal [*riferimento al contratto/ convenzione*] , la Regione Toscana – Giunta Regionale, in qualità di Titolare, nomina *[riferimento al soggetto individuato come Responsabile*], Responsabile del trattamento, ai sensi dell'articolo 28 GDPR.

I trattamenti affidati dal Titolare al Responsabile riguardano:
[

Descrizione sintetica dei trattamenti, descrivendo:
. le operazioni di trattamento
. la tipologia di dati trattati (dati comuni (es. anagrafici e di contatto, ecc…); dati sensibili (es. dati sanitari, genetici, biometrici, ecc…); dati giudiziari….)
. le categorie e numerosità degli interessati

Oppure riferimenti a parti del contratto/convenzione dove questi elementi sono descritti

]

I trattamenti effettuati per conto del Titolare dal Responsabile cesseranno al completamento del contratto/convenzione ovvero in caso di sua risoluzione, per qualsiasi altro motivo.
Se una disposizione del presente articolo è o diventa invalida o inapplicabile, la validità e l'applicabilità delle altre disposizioni del medesimo rimangono inalterate. In questo caso, Titolare e Responsabile concordano di adottare una disposizione che corrisponda al meglio allo scopo previsto nella disposizione non valida o agli interessi comuni.

[riferimento al soggetto individuato come Responsabile], in quanto Responsabile, fornisce garanzie sufficienti, in particolare in termini di conoscenze specialistiche, affidabilità e risorse, per attuare misure tecniche e organizzative che soddisfino i requisiti normativi sanciti dal GDPR, dal Codice Privacy e da qualsiasi altra norma connessa inerente al trattamento dei dati personali, comprese le misure di sicurezza del trattamento, per garantire la riservatezza e la protezione dei diritti degli interessati.
[riferimento al soggetto individuato come Responsabile], in quanto Responsabile, è tenuto ad assicurare e far assicurare ai propri dipendenti, collaboratori e responsabili ulteriori, la riservatezza ed il corretto trattamento delle informazioni, dei documenti e degli atti amministrativi, dei quali venga a conoscenza durante l'esecuzione della prestazione.
In tal senso il responsabile, si impegna a consegnare, alla firma del *contratto/convenzione*, al Titolare e al DPO della Giunta Regionale Toscana "il disciplinare di comportamento degli autorizzati e degli altri dipendenti" coinvolti in modo e diretto o indiretto nella esecuzione dei trattamenti svolti per conto del Titolare e delle istruzioni impartite agli autorizzati nei loro relativi ruoli *(solo nel caso in cui il Responsabile abbiam propri autorizzati)*.

In particolare, ai sensi dell'art. 28 GDPR, *[riferimento al soggetto individuato come Responsabile*] si impegna a:

1. adottare e mantenere aggiornato un proprio registro dei trattamenti, concordandone la struttura e le modalità di aggiornamento, con il DPO della Giunta Regionale Toscana entro 30 giorni dalla firma del contratto/convenzione. *(solo nel caso in cui il Responsabile ricada nelle fattispecie previste dal GDPR)*
2. non mettere in atto, per nessun motivo, trattamenti di dati diversi da quelli autorizzati dal Titolare oggetto del presente contratto/convenzione e presenti, se sia adottato, nel registro dei trattamenti. In tal senso renderà accessibile al Titolare il registro dei trattamenti, attivati per effetto del contratto/convenzione, consentendo operazioni di consultazione, approvazione e diniego in relazione a singoli o gruppi di trattamenti.
3. fornire per iscritto agli autorizzati al trattamento le necessarie istruzioni in tema;
4. nominare gli autorizzati che svolgono le funzioni di "amministratore di sistema", ai sensi dei provvedimenti del Garante italiano per la protezione dei dati personali del 27/11/2008 e del 25/6/2009, conservando i relativi estremi identificativi, definendo gli ambiti di operatività ai medesimi consentiti e comunicandone al titolare l'elenco nominativo con i relativi ambiti di operatività;
5. di collaborare alla eventuale redazione di DPIA su trattamenti affidati alla sua responsabilità dal Titolare;
6. predisporre e trasmettere, con cadenza annuale e comunque ogni qualvolta ciò appaia necessario, al Titolare Regione Toscana – Giunta Regionale - una relazione in merito

agli adempimenti eseguiti e alle misure di sicurezza adottate al fine di renderle e mantenerle sempre adeguate ed aggiornate rispetto alla evoluzione delle minacce e sulla base dei riscontri derivanti dalla registrazione continua e puntuale degli incidenti eventualmente occorsi;

7. assistere e garantire il titolare del trattamento nell'evasione delle richieste e del rispetto dei tempi previsti, nei rapporti con l'Autorità Garante per la protezione dei dati personali,
8. assistere il Titolare al fine di dare seguito alle richieste per l'esercizio dei diritti degli interessati ai sensi degli artt. 15 a 22 del Regolamento UE; qualora gli interessati esercitino tale diritto verso il Responsabile, quest'ultimo è tenuto ad inoltrare tempestivamente e comunque nel più breve tempo possibile, le istanze al Titolare, supportando quest'ultimo al fine di fornire adeguato riscontro agli interessati nei tempi prescritti,
9. assistere ed assicurare la piena, fattiva e puntuale collaborazione al titolare del trattamento, ed in particolare al Security IT Manager del Titolare se nominato, nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR, tenendo conto della natura del trattamento, della tipologia di dati trattati, delle categorie e numerosità degli interessati,
10. garantire al Titolare, su richiesta, l'accesso e la disponibilità permanente ai dati, su formati e strumenti di uso comune che ne garantiscano la fruizione da parte del titolare, consentendo in tal modo la piena continuità dei servizi oggetto del presente appalto e in modo che mai si configuri una situazione di lock in. Il titolare deve essere sempre messo in condizione di poter garantire la continuità del servizio,
11. Tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, il Responsabile del trattamento deve mettere in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio e per garantire il rispetto degli obblighi di cui all'art. 32 del Regolamento UE. Tali misure comprendono tra le altre, se del caso

    [

    personalizzare, ove necessario, in ragione dell'oggetto del contratto

    a. *la pseudonimizzazione e la cifratura dei dati personali;*
    b. *la capacità di assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi che trattano i dati personali;*
    c. *la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;*
    d. *una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;*
    e. *altro*

    ]

A tal fine si impegna ad assistere ed assicurare la piena, fattiva e puntuale collaborazione al titolare del trattamento, ed in particolare al Security IT Manager del Titolare.

1. *[Solo se sussiste l'esigenza]* Restituire tutti i dati personali di pertinenza del Titolare, dopo che è terminata la prestazione dei servizi relativi al trattamento, cancellando le

copie esistenti in proprio possesso, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati. In tal senso entro 120 giorni dalla firma del *contratto/convenzione [riferimento al soggetto individuato come Responsabile]* e il responsabile del *contratto/convenzione* per la Regione Toscana, concordano modalità, tempi e forme idonee a garantire il non precostituirsi di situazioni di lock in, inteso come la diminuzione o perdita della possibilità da parte del Titolare di garantire i servizi, senza ricorrere forzatamente al soggetto Responsabile, e di gestire agevolmente, in modo sicuro e con tempi ragionevoli, la chiusura del *contratto/convenzione* e l'eventuale subentro di un nuovo contraente o la gestione in autonomia in toto o in parte dei servizi. Tale accordo documentato viene messo a disposizione del Titolare e del DPO della Giunta regionale;

2. il Responsabile informa tempestivamente e, in ogni caso senza ingiustificato ritardo dall'avvenuta conoscenza, il Titolare di ogni violazione di dati personali (cd. data breach); tale notifica è accompagnata da ogni documentazione utile, ai sensi degli artt. 33 e 34 del Regolamento UE, per permettere al Titolare del trattamento, ove ritenuto necessario, di notificare questa violazione all'Autorità Garante per la protezione dei dati personali, entro il termine di 72 ore da quanto il Titolare ne viene a conoscenza; nel caso in cui il Titolare debba fornire informazioni aggiuntive all'Autorità di controllo, il Responsabile supporterà il Titolare nella misura in cui le informazioni richieste e/o necessarie per l'Autorità di controllo siano esclusivamente in possesso del Responsabile e/o di suoi sub-Responsabili;
3. Sarà obbligo del Titolare del trattamento vigilare durante tutta la durata del trattamento, sul rispetto degli obblighi previsti dalle presenti istruzioni e dal Regolamento UE sulla protezione dei dati da parte del Responsabile del trattamento, nonché a supervisionare l'attività di trattamento dei dati personali effettuando audit, ispezioni e verifiche periodiche sull'attività posta in essere dal Responsabile. A tal fine il Responsabile del trattamento metterà a disposizione, su richiesta del titolare del trattamento, tutte le informazioni necessarie per dimostrare il rispetto degli obblighi derivanti dal regolamento UE, agevolando il contributo alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato, ivi compresa, se necessario, l'attività di monitoraggio e controllo da parte del DPO e del Security IT Manager (se nominato), sulle misure di sicurezza attuate e sulla loro efficacia fornendo tutta la documentazione che sarà richiesta e collaborando attivamente alle attività di rilevazione e misura.
4. Comunicare al Titolare il nome ed i dati del proprio "Responsabile della protezione dei dati" (DPO), qualora, in ragione dell'attività svolta, ne abbia designato uno conformemente all'articolo 37 del Regolamento UE; il Responsabile della protezione dei dati personali (DPO) del Fornitore/Responsabile collabora e si tiene in costante contatto con il Responsabile della protezione dei dati (DPO) del Titolare
5. Comunicare al Titolare, al DPO *e al Security Manager (se nominato*) il nome e i riferimenti di contatto del proprio Responsabile della sicurezza IT,
6. Mettere in atto gli interventi necessari qualora l'attività di monitoraggio e controllo mettesse in evidenza punti di debolezza nelle misure e nelle tecniche adottate o qualora durante l'esecuzione del Contratto, la normativa in materia di Trattamento dei Dati Personali generi nuovi requisiti (ivi incluse nuove misure di natura fisica, logica, tecnica, organizzativa, in materia di sicurezza o trattamento dei dati personali), il

Responsabile del trattamento si impegna a collaborare - nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse - con il Titolare affinché siano sviluppate, adottate e implementate misure correttive di adeguamento ai nuovi requisiti;

7. *[Solo se sussiste l'esigenza*] Fornire e a mantenere aggiornato il catalogo degli asset (comprese le applicazioni utente e quelle di gestione dei sistemi e degli apparati), delle minacce e delle misure di sicurezza adottate e delle loro correlazioni al fine di una agevole valutazione dei rischi in fase di DPIA. A tal fine Titolare concorda entro 30 giorni dalla firma del contratto/convenzione, con il responsabile di contratto e il Security IT Manager (se nominato) oppure con il responsabile della sicurezza del committente, i contenuti e i formati dei cataloghi al fine della condivisione e l'aggiornamento di tali informazioni.
8. *[Solo se sussiste l'esigenza*] fornire al Titolare e al DPO per il tramite del responsabile di contratto/convenzione il proprio piano di qualità di esecuzione della fornitura dei servizi, contenente le misure tecniche, organizzative e di processo. al fine di fare fronte ai principi del GDPR con riferimento particolare all'accountability, alla Data Protection by Design e by Default, alla tenuta del registro dei trattamenti, alla garanzia del rispetto dei diritti degli interessati di cui al Capo III del regolamento e alla consapevole responsabilizzazione del proprio personale coinvolto nel trattamento dei dati, che avviene per conto del Titolare.

[solo nel caso della presenza di sub responsabili]

Nel caso in cui per le prestazioni affidate dal Titolare al Responsabile, quest'ultimo ritenga di avvalersi di ulteriori soggetti, è obbligato a nominarli quali sub-responsabili del trattamento, assicurandosi che il sub-responsabile presenti garanzie sufficienti in termini di competenza e conoscenza specialistica, affidabilità e risorse per l'adozione di misure tecniche e organizzative appropriate di modo che il trattamento dei dati risponda ai principi e alle esigenze del GDPR, e deve:

1. sottoporre a preventiva autorizzazione scritta e specifica del Titolare qualsiasi affidamento di trattamenti ad ulteriore responsabile (cd. "sub-responsabile");
2. far rispettare obblighi analoghi a quelli forniti dal Titolare al Responsabile del trattamento, riportati in uno specifico contratto o atto di nomina. Qualora il sub-responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile conserva nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi del sub-responsabile
3. *[solo nel caso in cui il Responsabile abbia già identificato il sub Responsabile]* far adottare agli eventuali sub-responsabili, idonee e preventive misure di sicurezza tecniche ed organizzative appropriate, atte ad eliminare o, comunque, a ridurre al minimo qualsiasi violazione, rischio di distruzione o perdita, anche accidentale, dei dati personali trattati, di accesso non autorizzato o di trattamento non consentito o non conforme, nel rispetto delle disposizioni contenute nell'articolo 32 del GDPR;

I trattamenti affidati dal Responsabile al sub responsabile riguardano:

[

Descrizione sintetica dei trattamenti, descrivendo:
. le operazioni di trattamento

. la tipologia di dati trattati (dati comuni (es. anagrafici e di contatto, ecc…); dati sensibili (es. dati sanitari, genetici, biometrici, ecc…); dati giudiziari….)
. le categorie e numerosità degli interessati
. altro

]

ART 2 - Penali

Nel caso in cui il Responsabile agisca in modo difforme o contrario alle legittime istruzione del Titolare oppure adotti misure di sicurezza inadeguate rispetto al rischio del trattamento risponde del danno causato agli "interessati". In tal caso, il Titolare potrà risolvere il contratto/convenzione, salvo il risarcimento del maggior danno.

Data e Firme …

Allegato F

Clausole Contrattuali Contitolarità

Data Protection Agreement

1 Scopo del documento

Il presente documento ha per obiettivo quello di fornire un facsimile di accordo Data Protection (Data Protection Agreement) nel caso in cui la relazione che si viene ad istaurare per il trattamento di dati personali sia fra due soggetti o più soggetti, che a norma del GDPR si possano classificare come Contitolari rispetto ai trattamenti nei quali vengono coinvolti dati personali.

Si tratta di due o più soggetti giuridicamente diversi che concorrono ognuno per proprie parti all'interno di una unica finalità e determinano congiuntamente i mezzi attraverso i quali eseguire i trattamenti di dati personali. Questi soggetti pertanto devono sottoscrivere un accordo, nel quale si da atto degli impegni comuni e comune responsabilità, nell'eseguire trattamenti all'interno di un preciso processo che prevede il trattamento di dati personali.

Il facs simile che segue, deve essere ovviamente compilato e personalizzato sulla base di quanto e come ogni soggetto contribuisce al processo complessivo, pertanto costituisce una linea guida nella formalizzazione dell'accordo.

L'articolato che segue può essere oggetto di uno specifico accordo od essere inserito all'interno di atti convenzionali o protocolli di intesa che vengono sottoscritti per regolare anche altri rapporti oltre alla Data Protection.

80 Fac-simile di Accordo Contitolarità

Accordo di contitolarità
(Data Protection Agreement)

Tra

La REGIONE TOSCANA- Giunta Regionale , con sede in _____, rappresentata dal dirigente del [*Settore/direzione]* _____,
Dott._____,nella sua qualità di delegato del titolare del trattamento

E

[Titolare 1], con sede in _____, rappresentata da_____,
Dott._____, nella sua qualità di _____

E

[Titolare 2],, con sede in _____, rappresentata da_____,
Dott._____, nella sua qualità di _____

(di seguito, congiuntamente, i *"Contitolari"*)

Premesso che:

- Il Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, applicabile definitivamente a tutti gli stati membri dal 25 maggio 2018, ha introdotto varie novità tra le quali assume particolare rilievo l'approccio basato sul principio di accountability inteso come elemento di responsabilizzazione dei soggetti coinvolti nel trattamento dei dati;

- Il Titolare del trattamento dei dati personali, in continuità con il D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali", come modificato dal Decreto Legislativo 10 agosto 2018, n. 101, rappresenta, nell'ambito del quadro normativo in materia di protezione dei dati, il soggetto a cui competono le decisioni relative alle finalità e ai mezzi del trattamento;

- Il Regolamento UE non esclude la possibilità che in talune circostanze uno o più soggetti possano determinare congiuntamente le finalità e i mezzi del trattamento dei dati. In tal senso si esprime l'art. 26 del Regolamento UE che configura tali soggetti quali "contitolari" del trattamento con rispettive responsabilità da ripartire e definire in modo trasparente in un *accordo* interno;

- come evidenziato anche dal parere n. 1/2010 del WP29 sussiste la contitolarità *"quando varie parti determinano, per specifici trattamenti, o la finalità o quegli aspetti fondamentali degli strumenti che caratterizzano il titolare del trattamento"* tenendo conto che *"la partecipazione delle parti alla determinazione congiunta può assumere varie forme e non deve essere necessariamente ripartita in modo uguale";*

- In relazione a quanto delineato dal parere n. 1/2010 WP29 e all'interpretazione letterale dell'art. 26 del Regolamento UE 2016/679, i rapporti tra contitolari possono quindi articolarsi in modo *asimmetrico,* nel senso che in alcune situazioni i soggetti coinvolti possono determinare in misura diversa le finalità e/o i mezzi e conseguentemente ciascuno di essi risponde solo per una parte del trattamento;

Richiamati:
[
Richiamare in elenco la legge/regolamento/atto/contratto/progetto….che definiscono la base di liceità, le finalità e le attività di trattamento oggetto dell'accordo per i contitolari
]
Considerato che:

- il nuovo quadro normativo ed in particolare il Regolamento UE 2016/679 concede ai Titolari del trattamento maggiore autonomia, ma allo stesso tempo maggiori responsabilità in applicazione del principio di accountability che richiede di **comprovare,** anche tramite evidenze, le valutazioni, le scelte e le misure adottate a garanzia della protezione dei dati personali;

- Il Regolamento UE 2016/679 presuppone quindi la definizione di un modello "organizzativo" con ruoli, compiti e responsabilità dei vari attori coinvolti nelle attività,

nonché del perimetro di azione di ciascun soggetto per quanto riguarda il trattamento e la gestione di dati personali;

SI CONCORDA QUANTO SEGUE

Art 1
Pemesse, richiami e considerata

Le premesse, i richiami e i considerata costituiscono parte integrante del presente Accordo.

Art 2
Oggetto dell'accordo

Il presente accordo di contitolarità regolamenta l'ambito di azione e le responsabilità dei contitolari del trattamento in merito all'osservanza degli obblighi derivanti dal Regolamento UE 2016/679 , compreso il rapporto con le categorie dei soggetti i cui dati saranno oggetto del trattamento. In particolare l'accordo ha lo scopo di definire i compiti dei contitolari relativamente alle attività di trattamento dei dati personali riconducibili a ciascuno di essi.

Art. 3
Attività di trattamento dei dati personali di ciascun contitolare

Il Regolamento UE 2016/679 insiste sulla necessità di delineare con chiarezza i ruoli, i compiti e le responsabilità per garantire principalmente i diritti delle persone interessate (soggetti a cui si riferiscono i dati personali).
Come descritto in premessa, quando due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento essi sono *contitolari* e in quanto tali sono tenuti, ciascuno per la propria parte, ad adottare le relative misure, tecniche e organizzative, per garantire la protezione dei dati personali.

I Contitolari svolgono i propri compiti nel rispetto dei principi di finalità, di proporzionalità e di minimizzazione dei dati personali trattati e trattano i dati degli interessati (persone fisiche) congiuntamente come di seguito descritto per una migliore gestione delle attività finalizzate alla realizzazione delle finalità di ciascuno.

A tal fine si specifica quanto segue:

La **Regione toscana - Giunta regionale** nell'ambito del presente accordo di contitolarità ha il compito di:
[
Descrivere i compiti svolti

]

Tali funzioni comportano il trattamento dei seguenti dati personali (specificare la tipologia di dati, le categorie degli interessati e la loro numerosità atta ad individuare se trattasi di trattamento su larga scala):
[

- …..
- …..
- ….
-

]
e lo svolgimento delle seguenti operazioni di trattamento:
[
- …..
- …..
- ….
-

]

Il [Titolare 1] nell'ambito del presente accordo di contitolarità ha il compito di:
[
Descrivere i compiti svolti

]
Tali funzioni comportano il trattamento dei seguenti dati personali (specificare la tipologia di dati, le categorie degli interessati e la loro numerosità atta ad indivduare se trattasi di trattamento su larga scala)::
[
- …..
- …..
- ….
-

]
e lo svolgimento delle seguenti operazioni di trattamento:
[
- …..
- …..
- ….
-

]

[ripetere per ogni titolare che concorre all'accordo di contitolarità]

Art. 4
Modalità di trattamento

La **Regione toscana - Giunta regionale** tratterà i dati con modalità Cartacea [descrizione sommaria del processo e dei trattamenti di cui è composto] e/o digitale, attraverso i seguente applicativo_____ *[descrizione sommaria del processo di trattamento]*_____

Il *[titolare 1]* tratterà i dati con modalità Cartecea [descrizione sommaria del processo di trattamento] e/o informatizzata, attraverso i seguente applicativo_____ [*descrizione sommaria del processo e dei trattamenti di cui è composto]*_____

[ripetere per ogni titolare che concorre all'accordo di contitolarità]

Schema riassuntivo dei dati trattati, delle finalità e modalità del trattamento

Contitolarità del trattamento	Categoria di interessati	Tipologia dei Dati	Finalità del trattamento	Modalità del trattamento

Art. 5
Ambito di comunicazione

I contitolari si impegnano ad istruire ed autorizzare le persone fisiche facenti parte della propria organizzazione a trattare i dati personali e a nominare, laddove sussistono i presupposti, come responsabili del trattamento i soggetti esterni che potrebbero eventualmente intervenire nelle operazioni di trattamento per conto dei contitolari stessi. Precisamente, i dati di natura personale potranno essere comunicati a destinatari appartenenti alle seguenti categorie:

a) soggetti che forniscono servizi per la manutenzione/gestione del sistema informativo e delle reti di telecomunicazioni ;
b) autorità competenti per adempimenti di obblighi di legge e/o di disposizioni di Autorità pubbliche, su richiesta.

80.1.1

In caso di trasferimento dei dati all'esterno dell'Unione Europea, i dati dovranno essere trattati nei limiti e alle condizioni del Regolamento UE 2016/679.

Art. 6
Informativa Privacy

Il [*indicare il contitolare/i che raccoglie i dati]si impegna a fornire, in sede di raccolta del dato, le informazioni di cui all'art. 13 del Regolamento UE 2016/679. Nello specifico*

l'informativa privacy verrà inserita nella piattaforma/sito web/modulo cartaceo/ affissa in luogo accessibile al pubblico…, consentendo ai soggetti interessati di prenderne visione.

Art.7
Esercizio dei diritti dell'interessato

Tutte le richieste di esercizio dei diritti di cui agli artt. 15-22 del Regolamento UE 2016/679 saranno gestite, per conto e nell'interesse di tutti i Contitolari, dal_____(*dati di contatto del contitolare indicato*), rivolgendosi al **Responsabile della Protezione dei Dati (DPO),** contattabile all'indirizzo mail: _____ *[o altro canale di comunicazione/contatto]*.

Art 8
Sicurezza del trattamento

Nel rispetto dei principi di cui all'art. 32 del Regolamento UE 2016/679 i contitolari nei limiti delle funzioni esercitate e delle rispettive prerogative, tenendo conto anche dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità di trattamento, adottano misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio (es. misure atte a garantire su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento).

Nel valutare l'adeguato livello di sicurezza i singoli contitolari devono tenere conto dei rischi di:

- Perdita;
- Distruzione;
- Modifica;
- Divulgazione non autorizzata;
- Accesso accidentale o illecito a dati personali trasmessi, conservati o comunque trattati.

I Contitolari, in quanto parti dell'Accordo si impegnano a stabilire, attuare, mantenere e migliorare un sistema di gestione per la sicurezza delle informazioni, sia con riferimento a strumenti, archivi e supporti cartacei, sia con riferimento a strumenti e mezzi digitali e informatici utilizzati.

Art. 9
Data Breach

Si intende per Data Breach ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati dal titolare del trattamento.

Ai sensi e per gli effetti dell'art. 33 Regolamento UE 2016/679, il titolare del trattamento, in caso di violazione di dati personali, notifica la violazione all'autorità di controllo competente senza ingiustificato ritardo e ove possibile entro 72 ore dal momento in cui ne è venuto a conoscenza a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica non sia effettuata entro 72 ore è corredata dai motivi di ritardo. Ai sensi e per gli effetti dell'art. 34

Regolamento UE 2016/679, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo qualora la violazione di dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà fondamentali dell'interessato.

Titolare del trattamento per la gestione di eventuali Data Breach è _____, il quale si atterrà alla disciplina per la gestione delle violazioni dei dati. Ciascun contitolare dovrà pertanto comunicare tempestivamente al _____ gli eventuali casi di data breach per la valutazione congiunta del fenomeno e per le eventuali comunicazioni al Garante e agli interessati.

Art. 10
DPIA

Per ogni nuova iniziativa che comporti l'utilizzo di nuove tecnologie per il trattamento dei dati, o in caso di modifiche di strumenti del trattamento già adottati (art. 35 s.s. Regolamento UE 2016/679 – art. 23 e 24 D.Lgs. 51/2018), i Contitolari si impegnano a collaborare per la valutazione dei rischi connessi e delle misure tecniche ed organizzative da adottare a tutela dei dati personali.

Art. 11
Conclusioni

Le parti si impegnano a revisionare il presente accordo in caso di necessità; a tal fine verrà monitorato e revisionato periodicamente per assicurarne l'attualità e l'allineamento alle novità legislative.
Il presente accordo viene meno con il conseguimento delle finalità del trattamento da parte dei contitolari o qualora non vi siano più i presupposti di contitolarità.
Ai sensi dell'articolo 26 comma 2 del Regolamento UE 2016/679, il contenuto essenziale del presente accordo sarà pubblicato sul sito del _____ e in tal modo messo a disposizione degli interessati.

Luogo, data, firme

Allegato G

Registro delle Attività di Trattamento
Linee Guida

1 Scopo del Documento

Queste linee guida riprendono quanto formalizzato attraverso le indicazioni per la tenuta del registro dei trattamenti approvate con delibera di Giunta nr. 585/2018. Si rimanda alla lettura delle stesse al fine della contestualizzazione delle presenti linee guida.
Inoltre costituiscono parte integrante delle linee guida “Protection By Design/ By Default”.

81 Premesso

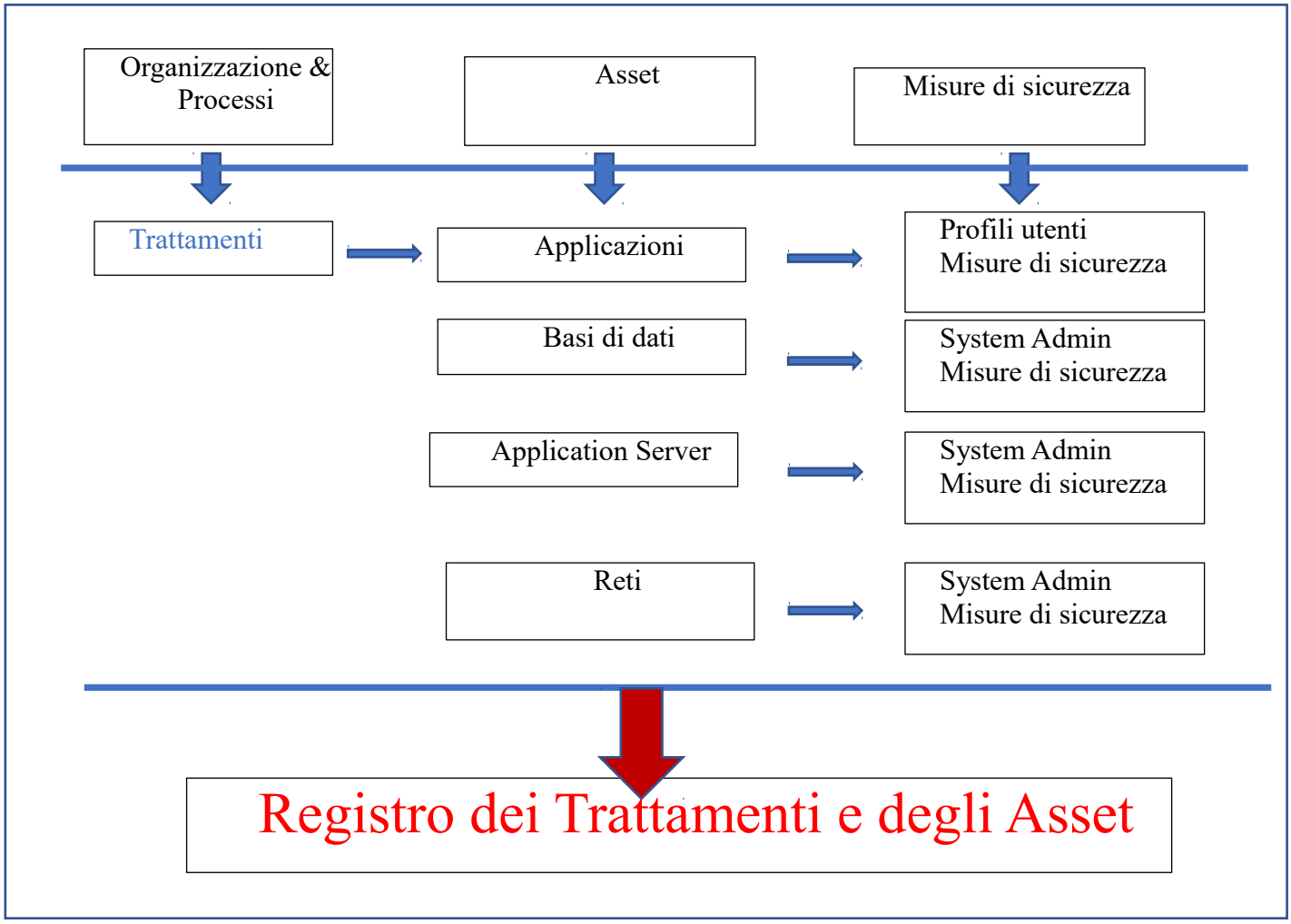
Il registro dei trattamenti viene ad essere una componente di un sistema che lega l’organizzazione dell’ente, i processi produttivi dello stesso, i trattamenti, gli asset tecnologici o meno e le persone titolate ad operare sulla base di specifici profili applicativi. Legare fra di loro questi elementi consente di mantenere aggiornata la struttura del registro rispetto alle variabilità:

1. degli assetti organizzativi, cambiamenti delle strutture e delle persone chiamate a ricoprire ruoli, funzioni e responsabilità
2. dell’evoluzione tecnologica e relative misure di sicurezza
3. del personale assegnato a funzioni di system amministrator
4.

L’attribuzione di profili applicativi per l’accesso alle applicazioni da parte dei delegati del titolare dei trattamenti (dirigenti) e l’attribuzione delle funzioni di system admin alle persone da parte dei delegati del titolare dei trattamenti (dirigenti) derivanti dalla gestione di asset, configurano queste persone come autorizzate a norma del GDPR e pertanto riportate sul registro dei trattamenti.

Qualora il sistema non consenta o ancora non consenta questi automatismi gli autorizzati devono essere individuati e registrati a cura del titolare o suo delegato.

Nello schema successivo vengono rappresentati gli elementi connessi ad ogni singolo trattamento.



82 Obiettivi del registro attività di trattamenti

Il registro dei trattamenti è previsto all'art.30 del GDPR (considerando 82) come misura fondamentale a carico del Titolare o suoi delegati, e del responsabile o sui delegati per rendere conto (principio dell' accountability) dell'attività e delle misure messe in atto ai fini della protezione dei dati personali, gestiti nella propria dall'organizzazione di cui hanno la rappresentanza legale.

Rappresenta quindi la porta di ingresso nell'organizzazione regionale per comprenderne il funzionamento e la idoneità delle misure tecniche e organizzative per garantire l'adeguato livello di protezione dei dati nonché la compliance (la conformità il rispetto) della normativa europea.
Diviene pertanto strumento di trasparenza nei confronti dell'autorità di controllo garante e strumento di partenza per indagini in caso di ispezioni, incidenti, denunce o quant'altro abbia una rilevanza giudiziaria.
Da questo l'importanza fondamentale di disporre di un registro dei trattamenti completo e sempre aggiornato.

Il regolamento europeo art. 83 e 84 prevedono sanzioni in merito al non rispetto degli obblighi derivanti dallo stesso e pertanto la cattiva gestione del registro da parte del titolare

risulterà l'elemento più visibile, in quanto punto di partenza di qualsivoglia ispezione o controllo.

83 Cosa è un trattamento

All'art. 4 del Regolamento europeo viene definito Trattamento qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Come si evince la definizione di trattamento si applica sia nel contesto di soluzioni IT sia in quello della gestione dei dati su carta o su un mix delle due soluzioni. Il trattamento è di norma un insieme di azioni che hanno come oggetto dati di natura personale diretta o indiretta. L'obbligo nasce anche verso quei dati che possono in qualche modo, anche se non direttamente, essere ricondotti alla persona fisica.

Il fatto che il trattamento possa essere un insieme di operazioni consente di avere un livello di aggregazione abbastanza alto al fine di contenerne il numero e collegarli ai processi dell'organizzazione.

84 Come lo si individua

La pubblica amministrazione opera e regola il suo operato su base di norme, che ne determinano le finalità e i suoi comportamenti, pertanto ogni trattamento deve avere una finalità e una norma di riferimento. Il punto di partenza per individuare i trattamenti all'interno di una direzione o settore della Regione sono i processi, cioè quell'insieme di attività che l'organizzazione pone in essere per il raggiungimento delle finalità, previste nelle norme che attribuiscono all'ente gli obiettivi da raggiungere e che l'ente stesso attribuisce alle diverse articolazioni organizzative.
Pertanto un processo può coinvolgere più strutture di una stessa organizzazione ma anche più enti quando questi sono emanazione della stessa al fine di migliorare l'efficienza e l'efficacia complessiva dell'azione pubblica.
Pertanto dato un processo, il trattamento è un segmento di quel processo attribuito da regole organizzative o dalle stesse norme alla competenza di uno specifico settore o direzione.
Stante l'organizzazione gerarchica regionale tutto ciò che non è attribuito alla diretta competenza del settore, ricade nell'ambito di competenza delle direzioni o della direzione generale.
Determinano quindi un trattamento: la struttura organizzativa competente, la finalità e la norma di riferimento, le azioni effettuate su archivi o insiemi di archivi.

85 La struttura del Registro dei Trattamenti

Premesso che un registro dei trattamenti si riferisce alla organizzazione di una figura giuridica e che pertanto devono essere indicati, oltre a tale dato anche:

a) il Titolare
b) il DPO
c) le regole di tenuta del registro stesso.

Il registro è composto da schede una per ogni trattamento articolate nelle seguenti sezioni:

a) Informazioni generali
b) Dettaglio del trattamento
c) Operazioni sui dati
d) Autorizzati

85.1Informazioni Generali

Questa sezione contiene:

a) La direzione competente e il direttore
b) Il dirigente (delegato del titolare) e la struttura di cui è responsabile con gli estremi di nomina
c) L'estensore, colui che materialmente per conto del dirigente gestisce la quota parte di competenza del registro o in assenza il dirigente stesso
d) La denominazione del trattamento
e) La descrizione del trattamento in termini di operazioni -che vengono svolte in relazione a quali archivi
f) L'esistenza o meno di un Responsabile (altra figura giuridica esterna all'organizzazione del titolare cui il titolare stesso affida lo svolgimento di operazioni del trattamento di sua competenza) [Nel caso sia presente la sezione contiene gli estremi identificativi del responsabile, e il DPO della figura giuridica del Responsabile se nominato, il contratto di servizio che lega il Titolare del Trattamento con il responsabile (questo può essere una sezione specifica del contratto di fornitura, una sezione di un atto convenzionale, o uno specifico atto bilaterale)]
g) L'esistenza o meno di uno o più Contitolari (altra o altre figure giuridiche che condividono stessa finalità e gli stessi mezzi) Nel caso di esistenza la sezione contiene: gli estremi indicativi del contitolare, del DPO e l'accordo (data Protection Agreement) che ne regola i rapporti, con particolare riferimento alle modalità di trasferimento o condivisione dei dati.
h) Se è prevista la trasmissione di dati verso paesi terzi o organizzazioni internazionali (Capo IV – art. 4, 45 e 46 GDPR) la sezione riporta l'identificazione dei soggetti, le finalità e la tipologia e riferimento ai dati oggetto del trasferimento.
i) Il riferimento al Dossier Data Protection nel quale sono contenuti tutti gli atti da cui deriva quel trattamento, la descrizione del processo di cui fa parte, eventuali DPIA, gli incidenti occorsi che hanno coinvolto il processo nel suo complesso, ecc..
j) Indicazione se il trattamento prevede la comunicazione di dati a terzi. In questo caso deve essere indicato il soggetto o i soggetti a cui vengono comunicati e la base normativa che prevede la comunicazione, il contratto/convenzione che regola i rapporti fra i soggetti, se esiste.

Questa sezione ha l'obiettivo, oltre che di individuare e descrivere il trattamento, di inquadrare le responsabilità in merito alle diverse figure previste dal GDPR, che entrano in gioco nel trattamento e acquisire gli elementi e le regole che governano le loro interazioni.

Inoltre aver legato il trattamento alle diverse istanze organizzative (direzioni/settori) consente nel caso di sostituzione delle persone alla responsabilità delle strutture organizzative o nel caso di revisione della organizzazione di attribuire automaticamente le responsabilità e relative deleghe ai dirigenti responsabili di settore o di direzione, o attribuire, in toto o in parte, trattamenti legati ad una specifica struttura organizzativa cessata o modificata, ad altra o altre.

85.2 Dettaglio trattamento

Questa sezione contiene in riferimento al trattamento e ha l'obiettivo di definire gli ambiti di applicazione del trattamento in termini di confini giuridici, dimensionali, temporali organizzativi e di rischio, collegando il trattamento ai processi produttivi dell'organizzazione e ai procedimenti amministrativi.

a) Le date di vigenza e validità del trattamento
b) La finalità principale del trattamento stesso da scegliersi fra un insieme preimpostato o inserirne una nuova
c) La legge di riferimento da cui discende la finalità
d) Altri fonti normative che sostengono o specificano la finalità del trattamento
e) Le finalità di particolare interesse pubblico da scegliere fra un insieme precodificato, nel caso in cui il trattamento preveda operazioni su categorie particolari di dati (art. 9 GDPR) o su dati giudiziari (art. 10 GDPR)
f) Le tipologie di soggetti/interessati coinvolti da scegliere fra un insieme precodificato
g) Le modalità del trattamento dei dati definite e correlate con l'analisi di rischio prevedendo un indicatore che sarà oggetto di valutazione e validazione da parte dell'ufficio del DPO.
h) Il processo di cui il trattamento fa parte, facendo riferimento al dossier data protection, da scegliere all'interno dell'insieme dei processi censiti con possibilità di inserirne di nuovi da sottoporre a valutazione dell'ufficio organizzazione e dell'ufficio del DPO
i) Il procedimento amministrativo correlato se esistente da scegliere fra un insieme precodificato per tipologia
j) La tipologia dei dati intesi come dati comuni, dati particolari (es. razziali, sanitari, religione, ecc..), dati giudiziari
k) Se i dati riguardano minori o altre categorie vulnerabili
l) Degli indicatori numerici in relazione ai soggetti interessati dal trattamento al fine di determinare se trattasi di trattamento su larga scala

85.3 Operazioni sui dati

Questa sezione descrive le operazioni e i mezzi attraverso i quali si svolge il trattamento. Nel caso in cui il trattamento sia processato da altra figura giuridica (il Responsabile) questa sezione non sarà presente nel registro del titolare ma lo sarà in quello del Responsabile

Contiene quindi:

a) Le operazioni sui dati con riferimento a quelle previste dal GDPR art.4
b) Le banche dati coinvolte nel trattamento, la loro interconnessione e le possibili interconnessioni con altre banche dati al fine di evidenziare la riconducibilità di dati alle persone fisiche
c) Se è stato chiesto il consenso o meno e se si quale modulo/i e modalità è stata utilizzata, se no la motivazione
d) Se è stata data l'informativa o meno se si, il modulo e la modalità, se no, la motivazione
e) Applicativo attraverso il quale si effettua il trattamento, l'applicativo in questione viene scelto attraverso l'archivio degli Asset. Applicazioni che possono sia essere interne all'organizzazione sia esterne.
f) La descrizione e localizzazione di archivi cartacei e le persone che vi hanno accesso
g) Se gli archivi sono localizzati su PC o su diversi PC e se del caso le persone che vi hanno accesso
h) Su rete interna (file server di rete) l'indicazione della directory e le persone che vi hanno accesso
i) Le informazioni da fornire all'autorizzato al trattamento

85.4Persone autorizzate al trattamento

In questa sezione sono riportate dinamicamente le persone che hanno ricevuto accesso ai sistemi o agli archivi e che pertanto sono autorizzate a determinate operazioni ~~azioni~~ nell'ambito del trattamento in questione, a norma del GDPR.
Pertanto le procedure organizzative devono prevedere che il rilascio di credenziali di accesso a sistemi, ad applicazioni, a cartelle di lavoro condivise siano richieste dal dirigente responsabile del trattamento a cui è finalizzata la richiesta di rilascio. (Si suggerisce di rivedere l'attuale modalità di richiesta di credenziali di accesso attraverso una unica procedura che sia in grado di tenere traccia delle richieste, dei tempi e delle persone richiedenti e autorizzate.)

In questa sezione pertanto vengono riportate le seguenti informazioni:

a) Codice fiscale,
b) nome e cognome
c) operazioni per cui è autorizzato collegata al profilo applicativo

Tali dati devono essere aggiornati in automatico o da immissione manuale in relazione ad asset tradizionali o derivandoli dai profili di accesso delle applicazioni o delle funzioni svolte in quanto amministratori di sistema o data base amministrator.

86 Il Catalogo degli Asset

Al fine della costituzione e aggiornamento tempestivo del Registro dei trattamenti viene istituito il Catalogo degli Asset.
Per Asset si vuole indicare quelle componenti strutturali tradizionali o innovative che sostengono le azioni sui dati che caratterizzano un trattamento.

Il catalogo degli Asset per le finalità del registro, ha i seguenti compiti:

a) Fornire le informazioni strutturate relative agli archivi e applicazioni quale supporto all'estensore nella compilazione delle sezioni "Dettaglio trattamento" e "Operazioni sui dati"
b) Aggiornare in automatico la sezione "Autorizzati" sulla base della concessione di credenziali di accesso associate ai profili applicativi, o di credenziali di accesso ai sistemi associati alle persone. Si ricorda che ogni sistema deve nascere chiuso, il suo accesso deve sempre essere regolato attraverso rilascio di credenziali autorizzate dal dirigente responsabile di quel trattamento o da livello gerarchico superiore.

Il ***catalog degli Asset*** di Regione Toscana contiene:

Anagrafica delle applicazioni contenente per ciascuna applicazione:

1. Descrizione, fornitore, interna o esterna ….
2. I profili applicativi e le relative azioni consentite
3. L'ambiente sistemistico attraverso le diverse componenti e relative release
4. Le misure di sicurezza
5. Gli incidenti occorsi e le azioni riparatrici

Anagrafica delle banche dati contenente per ciascuna:

1. Descrizione
2. Ambiente e relative release
3. Riferimento a Data dictonary
4. Misure di sicurezza
5. Data base amministrators

Anagrafica degli application server contenete per ciascuno:

1. Descrizione
2. Ambiente tecnologico e architetturale (fisico e virtuale)
3. Misure di sicurezza
4. Operazioni del System amministrator

Anagrafica dei contesti fisici e virtuali di rete

1. Descrizione
2. Ambiente tecnologico e architetturale
3. Misure di sicurezza
4. Operazioni del System amministrator

87 La Rete delle relazioni

Il basamento informativo all'interno del quale trova la sua collocazione il catalogo degli Asset è quindi composto dalle relazioni fra:

1) *Trattamenti e applicazioni*, ad un trattamento possono corrispondere una o più applicazioni ad ogni applicazione diversi profili di accesso che determinano le operazioni che gli utenti possono fare e gli utenti stessi che assumono la figura di autorizzati. Pertanto per ogni trattamento, inteso come gruppo di operazioni ,

corrispondono gli "autorizzati" ognuno con il proprio insieme di operazioni che il profilo associato rende possibile.

2) *Trattamenti e banche dati* quando queste *sono archivi cartacei* e pertanto non trattati da soluzioni/applicazioni IT. In questo caso devono essere comunque descritti i profili di accesso ed uso e associati alle singole persone nella loro funzione di autorizzati
3) *Applicazioni e banche dati,* relazione che descrive l'associazione fra le operazioni/azioni permesse dall'applicazione e i dati
4) *Applicazioni e Application server,* descrive il contesto architetturale tecnologico nell'ambito del quale l'applicazione viene ad inserirsi, derivando livelli di sicurezza e di operatività
5) *Application server e reti* , relazione che indica in quale contesto tecnologico e misure di sicurezza viene ad inserirsi l'ambiente applicativo..
6) *Trattamenti e Dossier Data Protection ,* ad un trattamento corrisponde un unico dossier , un dossier si riferisce a più trattamenti e contiene gli aspetti generali di contesto e gli accadimenti in merito ai trattamenti a cui si riferisce con particolare attenzione alla valutazione di impatto, alla gestione degli incidenti di sicurezza
7) *Trattamenti, strutture e persone:* un trattamento si riferisce ad una struttura competente, al titolare o responsabile, agli autorizzati. Indispensabile il collegamento con il sistema di gestione dell'organizzazione al fine dell'aggiornamento derivante da mutamenti organizzativi

Pertanto il registro dei trattamenti interrelato con il catalogo e la rete degli Asset e con il sistema di gestione organizzativa, costituisce il basamento informativo di conoscenza di come i dati sono collocati, utilizzati, e protetti.
Gli autorizzati quindi sono desunti: dal sistema IT di identificazione ed accesso, dalle persone addette alle funzioni di system amministrator dei diversi asset, dalle persone indicate come operatori su banche dati tradizionali.

88 Ambiti di competenza

Il titolare o suo delegato (Dirigente)
Ha il compito e responsabilità dei trattamenti a lui associati in quanto facenti capo, nell'ambito del modello organizzativo alla struttura di cui lui è responsabile per incarico. L'incarico di dirigente di una struttura pertanto ha come logica conseguenza la individuazione del dirigente, quale delegato del Titolare. In quanto delegato del titolare è sua responsabilità diretta la buona e corretta tenuta del registro dei trattamenti per quella parte attinente alla sua struttura.

Il responsabile dei sistemi informativi, ha il compito di mantenere aggiornato il catalogo degli asset relativi alle applicazioni e alle banche dati digitali e il collegamento di questi con gli asset infrastrutturali, reti e application server. Inoltre mantiene aggiornate le misure di sicurezza associate ai diversi asset (banche dati e applicazioni), oltre a trattamenti insiti nella gestione di tali asset (funzioni di system amministrator e relativi autorizzati).

Il responsabile delle infrastrutture ha il compito di mantenere aggiornato il catalogo degli asset infrastrutturali, relative misure di sicurezza oltre a trattamenti insiti nella gestione di tali asset (funzioni di system amministrator e relativi autorizzati).

L'Amministratore delle utenze che sulla base delle indicazioni del titolare o suo delegato, associa persone ai profili applicativi andando così a determinare le persone autorizzate alle diverse azioni del trattamento. Questa figura che può corrispondere ad una o più persone, si configura come autorizzato per il trattamento dell'archivio delle utenze, che deve essere censito alla pari di ogni altro trattamento da parte dei Titolari rappresentati dai dirigenti delle strutture competenti.

Amministratore di sistema / Data Base Amministrator , anche in questo caso la gestione di asset che comporta in maniera sistematica la possibilità di accesso o altre operazioni su dati personali deve essere ricondotta ad un trattamento e pertanto registrata nel Registro Trattamenti. Devono essere, se ci fossero individuati dei profili collegati all'applicazione di gestione dei sistemi, a loro volta assegnati ad una o più persone che vengono individuate come amministratori di sistema (autorizzati per quello specifico trattamento).

Qualora esista per l'una o l'altra componente un Responsabile tali obblighi vengono trasferiti allo stesso attraverso le indicazioni del titolare a cui il Responsabile deve attenersi.

89 Trattamenti specifici della gestione IT

La gestione di dati con l'ausilio di soluzioni IT comporta la individuazione di specifici trattamenti derivanti, non tanto dalle finalità del trattamento stesso, quanto dalla gestione dei sistemi all'interno dei quali o per loro mezzo si ha trattano dati personali.

A titolo esemplificativo:

Gestione delle utenze: rientrano in questo trattamento la raccolta dei dati personali di tutte le persone che a vario titolo accedono alle applicazioni e ai servizi IT, il loro collegamento ai profili, i file di log e quanto altro collegato a questa funzione.

Amministrazione di sistemi IT ivi compresi i DBMS: rientrano in questo argomento i trattamenti derivanti :

a) dall'organizzazione e strutturazione dei dati,
b) dalla condivisione di dati
c) dalle attività di back up e restore
d) dalle attività di gestione e manutenzione sistemi
e) dall'accesso ai dati per finalità di gestione

Amministrazione sistema Posta Elettronica, agende, lavoro di gruppo, piattaforme di collaborazione : rientrano in questo argomento i trattamenti derivanti:

a) gestione dei profili di utenza
b) dalle attività di Back up e Restore

c) dalle attività di gestione e manutenzione sistemi
d) dall'accesso ai dati per finalità di gestione e supervisione

Amministrazione di rete: rientrano in questo argomento i trattamenti derivanti:

a) gestione dei profili di utenza di accesso alle reti
b) assegnazione di indirizzi Ip a Persone Fisiche

Sviluppo e gestione applicazioni: rientrano in questo argomento i trattamenti derivanti:

a) accesso ai dati
b) duplicazione di dati fra sistemi di staging e di esercizio
c) manutenzione

90 Descrizione del processo di gestione

Uno dei principi generali del GDPR è la "Data Protecion By Design" di cui questo documento rappresenta una sua specificazione in merito ai trattamenti. Pertanto ci si riferisca al contesto generale descritto nelle linee guida Data Protection by Design per comprendere nell'ambito di quale processo nasce un nuovo trattamento o l'esigenza di modificarne uno esistente.

Il Trattamento è descritto e registrato sul registro in stato di bozza dal titolare o suo delegato (nel seguito comunque indicato con il termine Titolare) *nel momento in cui nasce l'esigenza* di un nuovo trattamento o della modifica di uno esistente.

a) Il Titolare registra o modifica la componente anagrafica del trattamento.
b) Viene inserito il riferimento al Dossier Data Protection di cui quel trattamento fa parte. In tale Dossier, se valutata l'esigenza, conterrà anche le risultanze della Valutazione di Impatto – DPIA- (vedi Linee Guida per l'effettuazione della DPIA)

Nelle fasi successive, in caso di trattamento che preveda l'ausilio di soluzioni IT il responsabile dello sviluppo dei sistemi informativi, tenuto conto delle valutazioni emerse in fase di valutazione dei rischi, provvede ad aggiornare eventualmente il catalogo degli asset applicativi e collegare questi a quelli infrastrutturali e ai trattamenti già registrati da parte del titolare.
Successivamente alla messa in esercizio della soluzione IT l'amministratore delle utenze procede ad assegnare persone ai rispettivi profili applicativi, in quanto autorizzati.
Un'applicazione non potrà in nessun caso essere posta in esercizio se la registrazione del trattamento non viene posta in stato di validata.
Il cambiamento di stato è competenza esclusiva del titolare che ha il compito di verificare la rispondenza della registrazione effettuata, alla realtà.
La Direzione competente è responsabile della coerenza e qualità della sezione di registro dei trattamenti relativi alle materie di sua competenza.

Il ciclo di vita del trattamento prevede elementi dinamici in relazione a:

1. *Persone autorizzate o cessate* (a cura dell'amministratore di sistema del sistema di autenticazione ed accesso)
2. *Misure di sicurezza adottate* (a cura del responsabile dei diversi Asset sotto la supervisione del responsabile dei sistemi informativi e del responsabile delle infrastrutture per i rispettivi ambiti di competenza, informando di questo il Security IT Manager)
3. *Profili applicativi. aggiunti o cancellati* (cura del system amministrator delle applicazioni)
4. *Cambiamenti di Titolare* dovuti a cambiamenti organizzativi, cessazioni di persone, ecc. (a cura del Direttore o Direttore generale o Avvocato Generale, in quanto responsabili dell'organizzazione di riferimento)
5. *Cambiamenti di Responsabile* (a cura del dirigente responsabile del contratto o convenzione)

Obiettivo fondamentale è quello di fare del Registro dei Trattamenti e delle relazioni di questo con gli asset, le persone autorizzate e i dossier data protection dei processi, il basamento informativo unitario di lettura delle politiche e degli strumenti di protezione dei dati in carico all'amministrazione regionale.

Allegato H

Classificazione dei Dati Personali

Linee Guida

1 Scopo del documento

Il presente documento vuole offrire una guida per identificare e classificare i dati personali in ambito Data Protection secondo quando previsto dal regolamento europeo 679/2016.

91 Premessa

La presente linea guida è redatta in coerenza con:

a) Il Regolamento Europeo 679/2016 relativo "alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati" (altrimenti detto GDPR);
b) "Article 29 Working Party - Guidelines on consent under Regulation 2016/679" adottato il 28 Novembre 2017 – ultima revisione del 10 Aprile 2018
c) Decreto legislativo 10 agosto 2018, n. 101 che adegua il Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196) alle disposizioni del Regolamento (UE) 2016/679.

L'articolo 1 del Regolamento (UE) 2016/679 (Oggetto e finalità) confina l'ambito di operatività del regolamento stesso alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alle norme relative alla libera circolazione di tali dati. Sottolinea inoltre che la finalità del regolamento è quella di proteggere i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali. Risulta quindi evidente che l'obiettivo primario è proteggere il dato personale e che la finalità è quella di proteggere i diritti e le libertà fondamentali delle persone fisiche.
Per garantire quindi una corretta applicazione del regolamento è fondamentale comprendere il significato di dato personale sapendolo individuare in ogni sua forma e/o rappresentazione.

92 Dato personale e trattamento

Riprendendo la definizione di «dato personale» (art. 4 - GDPR) : "qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale"
Si evince quindi che un dato personale è qualsiasi informazione che permette di ricondurci ad un singolo individuo attraverso le sue caratteristiche, le sue relazioni personali, le sue abitudini, il suo stile di vita e così via. In questa descrizione rientrano quindi tutte le informazioni cosiddette identificative (dai dati anagrafici alle immagini che ritraggono la persona), quelli cosiddetti particolari (dati sensibili) e quindi sottoposti a tutela particolare, e le informazioni giudiziarie che possono rivelare l'esistenza di determinati provvedimenti giudiziari a suo carico.

E' utile sottolineare che le nuove tecnologie digitali hanno esteso il concetto classico di dati personali includendo fra questi anche:

a) i dati relativi alle comunicazioni elettroniche via telefono o internet (es. un indirizzo IP);

b) i dati che consentono la geolocalizzazione della persona, fornendo informazioni su movimenti e luoghi frequentati;
c) i dati genetici
d) i dati biometrici.

I dati personali possono presentarsi sotto diverse forme: numeri e lettere dell'alfabeto (testo), immagini statiche (grafici, disegni, tratti) o in movimento (video), formati sonori (audio) o altro. Tali dati possono essere rilevati e poi conservati su diversi mezzi o supporti fisici (cartaceo, magnetico, ottico, etc) e/o veicolati (trasmessi) attraverso una rete di comunicazione tra più utenti che possono avere finalità differenti.

Da questi concetti, riprendendo in conclusione la definizione di "trattamento", riportata sempre all'interno del art.4 del regolamento : "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione" è subito chiaro che un trattamento è tale per il GDPR solo nel caso in cui lo stesso "processi" (in qualsiasi forma e con qualsiasi strumento) dati personali.

93 Identificazione diretta o indiretta

L'identificazione di un singolo individuo può essere possibile sia attraverso una "identificazione diretta" - utilizzando i dati anagrafici (ad esempio: nome e cognome), il codice fiscale, le immagini del proprio volto (ad alta definizione), ecc. – sia utilizzando dati che permettono una "identificazione indiretta", quali ad esempio un l'indirizzo IP, un numero di targa, un luogo e una data di nascita, un indirizzo di residenza, ecc.
Se appare evidente come un nominativo completo (es. Nome, Cognome e Codice Fiscale) possa identificare in modo certo ed univoco un individuo, spesso risulta più complesso capire come una serie di informazioni apparentemente non riconducibili ad un unico soggetto possano in realtà, se correlate e utilizzate in modo particolare, ricondurre comunque ad un singolo individuo.
Se infatti prendiamo alcune informazioni, quali ad esempio un semplice indirizzo di residenza e un anno di nascita che apparentemente non sembrerebbero ricondurre ad un soggetto e le correliamo fra di loro, potremmo invece scoprire essere informazioni in grado comunque di identificare (in taluni casi particolari) un singolo individuo qualora semplicemente a quell'indirizzo abitasse una persona con quell'età specifica.
Occorre quindi fare molta attenzione non solo ai dati che consentono una identificazione diretta dei soggetti ma anche a tutti quei dati che attraverso la loro elaborazione e/o correlazione possono comunque consentire l'identificazione di un soggetto in modo univoco.

94 Dati particolari

Tra i dati personali protetti dal nuovo Regolamento UE 2016/679 ve ne sono alcuni che sono oggetto di una maggiore tutela, in ragione della loro idoneità a rivelare aspetti connessi alla sfera più intima dell'individuo. Sono quelli che all'interno dell'art. 9 del GDPR sono definiti

"particolari" (definiti anche "particolarmente sensibili" all'interno dei considerano nr. 10 e nr. 51).
Il GDPR all'art. 9 infatti riporta: "È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona." Il divieto non si applica in presenza di consenso esplicito o di necessità per assolvere gli obblighi.
Le basi giuridiche che legittimano il trattamento dei dati particolari (art. 9 par. 2 GDPR) sono molteplici e specifiche fra cui le più rilevanti: la tutela di un interesse vitale dell'interessato; l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria; l'interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri; la necessità del trattamento in materia di diritto del lavoro, di protezione e sicurezza sociale o per finalità di medicina preventiva o medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi , assistenza o terapia sanitaria o sociale.

Il Dlgs 30 Giugno 2003 nr. 196 (ex Codice Privacy) come modificato dal Dlgs 101/2018 all'art. 2sexies, comma 1, stabilisce che la base giuridica per i trattamenti di categorie di dati particolar, per il settore pubblico, eè costituita esclusivamente da una norma di legge, o nei casi previsti per legge, da regolamenti che specifichino i tipi di dati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti e le libertà degli interessati.
E' quindi fondamentale comprendere quando si è in presenza di "dati particolari" sia per capire prima di tutto se il trattamento è lecito, e qualora questo lo sia, per applicare le corrette modalità di gestione (es. consenso esplicito e/o applicazione della base giuridica che legittima il trattamento dei dati particolari) e in ultimo per valutare l'adeguatezza del sistema di sicurezza e l'eventuale applicazione di ulteriori contromisure di sicurezza necessarie per la tutela di tali dati (es. cifratura).
Particolare attenzione va posta al trattamento del dato biometrico (oggetto di diversi provvedimenti sia da parte del Garante italiano sia del Gruppo di lavoro ex articolo 29) in considerazione del fatto che sono sempre più utilizzati strumenti per la raccolta di dati biometrici, quali impronte digitali, forma dell'iride, emissione vocale o firma grafometrica, a scopo di accertamento dell'identità personale, di accesso a servizi digitali e sistemi informativi o per finalità di controllo dell'accesso a locali.

E' utile sottolineare però, che il trattamento di fotografie non costituisce sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando sono trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica (tipicamente sistemi con immagini ad alta definizione).

95 Dati giudiziari

L'art. 10 del GDPR prevede che il "Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà

degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica".
Sono da considerarsi dati giudiziari tutti i dati relativi a condanne penali e reati cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato.

96 Ulteriori informazioni dell'Interessato

Oltre ai dati he si riferiscono all'interessato e che sono oggetto del trattamento occorre anche considerare la categoria di appartenenza dell'interessato e la numerosità degli interessati coinvolti nel trattamento, questo al fine di quantificare e qualificare i possibili danni derivanti da un incidente di data protection.
Per categorie di appartenenza degli interessati si intende: Minori, soggetti svantaggiati, soggetti appartenenti a categorie deboli, ecc
Per numerosità si intende se il trattamento si riferisce a pochi individui o ad una popolazione ad esempio di un comune, di una regione o ancora di dimensioni maggiore.
Risulta evidente che un trattamento che coinvolga dati particolari di una grande pluralità di soggetti per altro appartenenti a categorie deboli, richieda misure di sicurezza maggiori, di un trattamento che si riferisca a dati comuni per una popolazione ridotta di persone.
La valutazione dei rischi, delle minacce e degli effetti sugli interessati costituisce il ragionamento per individuare le misure di sicurezza più appropriate.

Allegato I

Data Protection Impact Assessment

Linee Guida

1 Scopo del documento

La presente Linea Guida definisce le principali responsabilità ed attività relative all'identificazione e valutazione degli aspetti connessi ai rischi derivanti dal trattamento dei dati personali, già in fase di definizione/progettazione/revisione dei processi dell'ente che comportano un nuovo trattamento di dati personali, in coerenza con il Regolamento Europeo 679/2016.
Ciò, in coerenza con quanto previsto dall'art. 35 par. 1 GDPR secondo il quale "Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali".
Per una più precisa identificazione di quando l'effettuazione di una DPIA, risulta obbligatoria si fa riferimento alle Linee-guida del Gruppo Articolo 29 in materia di valutazione di impatto sulla protezione dei dati (WP248)

Il presente documento descrive il processo di DPIA come sottoprocesso del più generale processo di Data Protection by design (vedi: linee guida Data Protection by Design).

La presente linea guida è redatta in coerenza con:

1. Il Regolamento Europeo 679/2016 relativo "alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati" (altrimenti detto GDPR);
2. le linee guida del Gruppo dei garanti (art.29) denominate "WP248 - Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento possa presentare un rischio elevato"
3. il Provvedimento del Garante per la protezione dei dati personali "Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679 - 11 ottobre 2018"
4. le "Indicazioni operative per la redazione di linee guida per la valutazione d'impatto del rischio (DPIA)" emesse da Regione Toscana il 23 maggio 2018.

Tale linea guida pertanto si applica a tutti gli archivi/documenti informatici e cartacei su cui sono conservati i dati personali degli interessati (Cittadini, dipendenti, fornitori, soggetti terzi ecc.) che la Regione e/o altri enti ad essa collegati trattano, anche attraverso il supporto di Responsabili del Trattamento.

97 Descrizione del Processo

L'attivazione di un nuovo trattamento o gruppi di trattamenti afferenti ad uno stesso processo o la modifica, richiede obbligatoriamente l'avvio del processo di Data Protection By Design (vedi le relative linee guida) nell'ambito del quale è prevista la decisione riguarda all'opportunità/obbligatorietà di effettuare una DPIA. Decisione che viene presa dal

titolare in considerazione degli obblighi di legge e della opportunità di effettuarla in base alla delicatezza dei dati trattati.
Nei casi e secondo le modalità previsti dalle norme, si procede alla ”consultazione preventiva dell’Autorità di Controllo”. Tale consultazione è da effettuarsi solo qualora la valutazione d’impatto sulla protezione dei dati di cui sopra rilevi un trattamento con rischio elevato e non siano state adottate misure per attenuarlo (Art. 36 (1)).

Per la gestione del processo di DPIA si è deciso di adottare quale strumento provvisorio la soluzione software “PIA” messa a punto dall’ autorità francese per la protezione dei dati (CNIL). Lo strumento PIA sarà poi affiancato da una o più soluzioni specifiche per l’elaborazione dell’analisi dei rischi in ambito sicurezza delle informazioni e dallo strumento per la gestione del registro dei trattamenti. Si evidenzia da subito l’esigenza di dotarsi di uno strumento più evoluto capace di collegarsi al registro dei trattamenti e al catalogo degli asset al fine di ereditare le misure di sicurezza adottate nei diversi contesti.
La procedura di DPIA si basa sui seguenti elementi:

a) I rischi
b) Le Minacce
c) Le Misure di sicurezza.

Per ciascuno dei primi due occorre valutare la “magnitudo” e la “probabilità”, in relazione al trattamento o insiemi di trattamenti in esame, questi due parametri danno la misura dell’effettiva gravità del danno. L’adozione di adeguate misure di sicurezza riduce la gravità del danno a quello che viene definito come rischio residuo.
Pertanto la procedura di DPIA ruota attorno a queste grandezze, alla loro misura e valutazione in relazione ai danni derivanti ai diritti e alle libertà individuali degli interessati.
Per ogni dettaglio e approfondimento relativamente al quadro normativo in cui si colloca il processo di Data Protection Impact Assessment, agli adempimenti prescritti dalla normativa, ai soggetti ed ai ruoli, ai casi di esenzione e di obbligo della DPIA, si deve fare riferimento al documento di “Indicazioni operative per la redazione di linee guida per la valutazione di impatto del rischio (DPIA)” pubblicate da Regione Toscana il 23 maggio 2018 che costituisce parte integrante del presente documento.

98 Ruoli e responsabilità

Ruolo / Struttura	***Responsabilità principali relative alla Procedura***
Titolare o Delegato del Titolare (Dirigenti / Direttori)	Descrivere (documentare) il trattamento/processo creando o aggiornando il Dossier Data Protection; Collaborare col il DPO nella verifica della conformità del trattamento e nella eventuale esenzione dall'obbligo della DPIA; Collaborare con il DPO nel processo di valutazione dell'impatto di Data Protection e nella formalizzazione delle decisioni prese (DPIA); Aggiornare il registro dei trattamenti in base alle decisioni prese nell'ambito della DPIA; nel caso in cui il trattamento preveda l'impiego di Sistemi Informatici e/o altri servizi da parte di Responsabili (esterni) richiedere contrattualmente l'invio dell'analisi dei rischi per la parte di trattamento esterno.
DPO	Collaborare con il Titolare o Delegato nella verifica di conformità del trattamento e nell'eventuale esenzione dell'obbligo della DPIA; Verificare se il trattamento richiede una valutazione di impatto sulla protezione dei dati (DPIA – Data Protection Impact Assessment); Collaborare alla DPIA, se richiesto, con il Titolare o Delegato del Titolare dei dati personali nell'ambito del trattamento di di sua competenza; Se necessario, richiedere all'Autorità di Controllo (Autorità Garante per la protezione dei dati personali) una consultazione preventiva sul trattamento in oggetto. Il DPO esprime un proprio parere in merito alla DPIA.
Security Manager	Effettuare l'analisi dei rischi sulla sicurezza del trattamento in ambito Data Protection; Valutare l'adeguatezza delle misure di sicurezza adottate per l'attuazione del trattamento, nel rispetto delle Security Policy e del Regolamento di Regione Toscana; Valutare l'eventuale esigenza di porre in atto misure di sicurezza aggiuntive, rispetto a quelle già previste per il trattamento in esame (revisione delle Security policy di base); Supportare il Titolare o suo Delegato nell'aggiornamento del documento DPIA relativamente ai risultati di Analisi dei Rischi e nella applicazione delle contromisure di sicurezza standard e/o aggiuntive adottate per la Protezione dei Dati.

Ruolo / Struttura	***Responsabilità principali relative alla Procedura***
Specialisti di Sicurezza/responsabile sistemi informativi/responsabile infrastrutture	Supportare il Security Manager nelle attività di Analisi dei Rischi fornendo tutte le informazioni necessarie al fine di valutare le vulnerabilità e le minacce a cui il trattamento può essere esposto e fornendo contestualmente le contromisure di sicurezza già presenti e/o applicabili al fine di mitigare i rischi in ambito Data Protection.
Responsabili	Garantire la valutazione delle contromisure standard e aggiuntive adottate per la Protezione dei Dati, per i Sistemi di competenza effettuati in qualità di Responsabili; Comunicare al Security Manager l'analisi dei rischi effettuata in qualità di Responsabili.

99 Procedura DPIA

La descrizione della procedura seguirà i passi previsti dal Software PIA attualmente adottato
Il primo elemento da comporre è :

Anagrafica della DPIA

a. Anagrafica DPIA;
b. Nome della DPIA;
c. Nome Autore (la persona incaricata di redigere la DPIA;
d. Nome Valutatore (il dirigente responsabile della struttura competente);
e. Nome Validatore (altra persona da individuare nell'organizzazione);
f. Data di creazione;
g. Nome del DPO.

Successivamente si procederà con i successivi passi sotto descritti ed infine:

h. Richiesta del parere degli interessati;
i. Motivazione della mancata richiesta del parere degli interessati;
j. Parere del DPO.

100 Descrizione Trattamento/Processo produttivo

A fronte della necessità di un nuovo trattamento, il Titolare o suo Delegato fornisce una descrizione del trattamento stesso compilando le sezioni preliminari specifiche contenute nello strumento PIA.

1) Informazioni di Contesto
   a) **Panoramica del trattamento**: Descrizione del processo complessivo a cui si applica la DPIA che dovrebbe essere già stata formulata al momento dell'apertura del Dossier Data Protection, se tale attività non fosse stata fatta occorre farla e aprire o aggiornare il dossier data protection (vedi linee guida Data Protection by Design);
      i) Descrizione del trattamento/processo;
      ii) Responsabilità in termini di figure GDPR e loro relazioni;

iii) Norme di riferimento da cui scaturisce la titolarità dei trattamenti;
iv) Applicazione di standard nazionali o internazionali.

2) Dati, processi e risorse di supporto
   a) **Descrizione dati trattati** anche questa componente descrittiva dovrebbe essere presente nel Dossier Data Protection, se tale attività non fosse stata fatta occorre farla e aprire o aggiornare il dossier data protection (vedi linee guida Data Protection by Design)
      i) **Dati trattati** indicando le categorie di dati trattati, le categorie degli interessati ai quali si riferiscono, la numerosità degli interessati coinvolti;
      ii) **Ciclo di vita dei dati** intendendo con questo le modalità di raccolta, conservazione e cancellazione e i relativi tempi;
      iii) Risorse a supporto dei dati.

101 Verificare la conformità al Regolamento

Il compilatore in collaborazione con il titolare, avvalendosi se necessario del supporto del DPO, verifica – compilando l'apposita sezione dello strumento software PIA – se:

1) il trattamento rispetta i princìpi applicabili al trattamento dei dati personali (CAPO II del Regolamento):
   a) Sezione "Proporzionalità e necessità":
      i) Scopi del trattamento;
      ii) Basi legali del trattamento;
      iii) Minimizzazione dei dati;
      iv) Correttezza e aggiornamento dei dati;
      v) Periodo di conservazione.

2) il trattamento rispetta i diritti degli interessati (CAPO III del Regolamento):
   a) Sezione "Misure a tutela dei diritti degli interessati":
      i) Informative;
      ii) Consenso;
      iii) Diritti degli interessati di accesso e portabilità;
      iv) Diritti degli interessati di limitazione e opposizione;
      v) Obblighi dei responsabili;
      vi) Trasferimento dei dati extra UE.

Una volta inserite da parte del soggetto compilatore, le sezioni vengono valutate dal responsabile della struttura competente e validate così come indicato nella parte anagrafica della DPIA. Il processo di validazione determina se il trattamento è "CONFORME" oppure no. Nel caso in cui il trattamento sia conforme si può procedere alla fase successiva.
Se l'esito di tale verifica risulta "NON CONFORME", il trattamento non può essere effettuato (fine processo).

102 Verificare obbligo / esenzione DPIA

Il Titolare del Trattamento con l'eventuale collaborazione del DPO rivedendo tutte le informazioni inserite nelle sezioni di descrizioni e conformità del trattamento verifica se:

a) Il trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche (Art.35,comma 1);
b) il trattamento ricade in una delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati (Art.35, comma 5);
c) il trattamento risulta già normato nel diritto vigente (Art.35, comma 10).

In particolare verifica che il trattamento non ricada all'interno di una o più casistiche presenti all'interno delle line guida del Gruppo dei garanti (art.29) denominate "WP248 (Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento) riprese e meglio specificate dal Garante Italiano all'interno del provvedimento n. 467 dell'11 ottobre 2018.

Nota:
Il Garante Nazionale con provvedimento n. 467 del 11 Ottobre 2018 (Pubblicato sulla Gazzetta Ufficiale n. 269 del 19 novembre 2018) ha individuato, così come previsto all'art. 35 comma 4 del GDPR, le tipologie di trattamenti per i quali la DPIA è un adempimento obbligatorio:

1. Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso App, relativi ad "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato.
2. Trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi).
3. Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.
4. Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).

5. Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn.3,7 e8).
6. Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).
7. Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogni qualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01 .
8. Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche
9. Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment).
10. Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.
11. Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.
12. Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

La decisione o meno di effettuare una DPIA e il suo svolgimento è in capo al titolare o suo delegato che si consulta con il DPO.

Nel caso in cui il trattamento ricada all'interno di almeno 2 dei casi esemplificativi riportati dalla linea guida WP248 o rientri nella casistica di cui al provvedimento del Garante n. 467/2018 la DPIA risulta obbligatoria.
In tutti gli altri casi è comunque responsabilità del Titolare valutare in base alla tipologia di trattamento se la DPIA è da effettuarsi o meno.

Nel caso in cui la DPIA non sia obbligatoria e non si ritenga comunque opportuno realizzarla, si procede ad aggiornare il Registro dei trattamenti con la decisione intrapresa, aggiornando con le informazioni raccolte fino a quel punto attraverso lo strumento "PIA" il Dossier Data Protection
In tale caso Il DPO conclude il processo valutativo con la sua firma ed espressione del proprio parere in merito.

103 Valutare aspetti di sicurezza del trattamento – Analisi dei Rischi

Il compilatore assistito dal Security Manager, dal responsabile della sicurezza delle infrastrutture e dal responsabile dei sistemi informativi, o loro delegati, avvalendosi se necessario del supporto di tecnici e specialisti, effettua una valutazione dei rischi e delle misure di sicurezza applicabili al trattamento/processo.

Nello specifico, attraverso l'utilizzo di appositi software di analisi dei rischi per la sicurezza delle informazioni, valuta aspetti di vulnerabilità e minacce a cui il trattamento può essere sottoposto attraverso l'applicazione di metodologie in linea con i principali standard internazionali (es. ISO31000, ISO27001, ISO27005).
Qualora il trattamento coinvolga ulteriori soggetti esterni (es. Responsabili) il Security Manager provvede a raccogliere le informazioni necessarie anche da tali soggetti (es. Analisi dei rischi esterne) per valutare i rischi del trattamento nella loro completezza.
Una volta individuati i principali rischi intrinseci a cui può essere sottoposto il trattamento il Security Manager verifica il livello di contromisure applicabili al trattamento stesso in base al suo collocamento all'interno delle infrastrutture di sicurezza fisiche, logiche ed organizzative della propria organizzazione.

In particolare, con l'ausilio dei risultati emersi dall'analisi dei Rischi:

a. Controlla che le misure e i meccanismi di sicurezza logica previsti nell'analisi dei rischi di Data Protection e derivanti dall'applicazione delle Security Policy siano effettivamente applicati nel caso in oggetto;
b. valuta se tali misure e meccanismi, posti in atto per affrontare i rischi per i diritti e le libertà degli interessati, siano sufficienti per garantire la protezione dei dati personali.

Se l'esito di tale valutazione è "RISCHIO ACCETTABILE", si riportano le informazioni di sintesi emerse dall'analisi dei rischi all'interno dell'apposita sezione dello strumento PIA e si procede alla formalizzazione delle decisioni assunte.
Se l'esito di tale valutazione è "RISCHIO NON ACCETTABILE", occorre procedere alla modifica delle Policy di sicurezza e/o alla valutazione di contromisure aggiuntive.

104 Modifica delle Policy di Sicurezza e contromisure aggiuntive

Qualora dalla prima Analisi dei rischi sia emerso un "RISCHIO NON ACCETTABILE" il Security Manager, avvalendosi del responsabile della sicurezza delle infrastrutture, del responsabile dei sistemi informativi e se necessario del supporto di tecnici e specialisti, effettua una valutazione della potenziale modifica delle Policy di sicurezza e delle eventuali misure di sicurezza aggiuntive che debbono essere applicate al trattamento per ridurre ulteriormente i rischi emersi per i diritti e le libertà degli interessati.
Nota bene: Le policy di sicurezza generali sono ricavabili dal catalogo degli asset, se asset già presenti. Qualora gli assett non fossero presenti in "archivio degli asset" o se non vi fossero associate le misure di sicurezza si procede all'aggiornamento di detto archivio.
Oltre quindi a valutare una revisione delle misure di sicurezza già in essere (estensione ed aumento dell'efficacia) valuta anche l'applicazione di ulteriori misure specifiche di Data Protection fra cui:

a. Eventuali tecniche di cifratura adottate;
b. eventuali tecniche di anonimizzazione adottate;
c. eventuali tecniche di pseudonimizzazione adottate;
d. misure di disaster recovery;
e. misure di business continuity;
f. controllo degli accessi.

Sempre con l'intento di impedire la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati.
Sulla base degli interventi aggiuntivi viene ricalcolata l'analisi dei rischi del trattamento applicando il nuovo livello di contromisure di sicurezza; se l'esito di tale valutazione è "RISCHIO ACCETTABILE", si riportano le informazioni di sintesi emerse dalla revisione dell'analisi dei rischi all'interno dell'apposita sezione dello strumento PIA e successivamente si procede alla formalizzazione delle decisioni assunte.
Diversamente, se l'esito di tale valutazione è "RISCHIO NON ACCETTABILE", occorre attivare un procedimento di consultazione preventiva con l'Autorità di Controllo.
La fine di questa fase viene sancita dalla firma del valutatore e del validatore e parere del DPO.

105 Richiedere consultazione preventiva

Nel caso in cui la valutazione d'impatto sulla protezione dei dati effettuata nel par. 5.5 indichi che il trattamento presenta un rischio residuo elevato, pur in presenza delle misure di sicurezza adottate, è necessario ricorrere alla consultazione dell'Autorità di Controllo (v. Art. 36, comma 1 del Regolamento).
In questo caso il DPO avvia e gestisce l'iter di consultazione come segue:

1) contatta l'Autorità di Controllo, richiedendo la consultazione preventiva;
2) predispone ed invia all'Autorità di Controllo tutte le informazioni relative al trattamento oggetto di consultazione, e cioè:
   a) Le rispettive responsabilità del Titolare del trattamento e dei Responsabili del trattamento se presenti;
   b) le finalità e i mezzi del trattamento previsto;
   c) le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del Regolamento;
   d) ove applicabile, i dati di contatto del titolare della protezione dei dati (DPO – art.37);
   e) i risultati della valutazione d'impatto sulla protezione dei dati effettuata;
3) fornisce all'Autorità di Controllo, su richiesta di questi, ogni altra informazione necessaria per la valutazione;
4) riceve dall'Autorità di Controllo il parere scritto relativo alla richiesta di consultazione;
5) condivide l'esito della consultazione con il Titolare o suo Delegato;
6) supporta il Titolare o suo Delegato nella valutazione dell'esito della consultazione e nelle decisioni conseguenti relative al trattamento stesso.

106 Formalizzare le decisioni prese e Registro dei trattamenti

Il Dossier del trattamento, prodotto attraverso l'utilizzo della soluzione "PIA", riassume l'esito delle verifiche e valutazioni effettuate fra cui:

a. Descrizione del trattamento;
b. verifica di Conformità;
c. verifica obbligo DPIA;
d. valutazione Sicurezza;
e. consultazione Preventiva.

Il DPO chiude il processo di DPIA apponendo la propria firma e parere.
Sulla base di tali elementi, il Titolare del Trattamento o suo Delegato, con l'ausilio del DPO, decidono se procedere o meno al trattamento.
Nel caso in cui si decida di procedere al trattamento il Titolare o uso Delegato provvederanno inoltre ad aggiornare il Registro dei Trattamenti, inserendo tutte le informazioni necessarie al suo censimento e aggiornando il Dossier Data Protection con i risultati della DPIA (Report DPIA ottenuto dalla procedura).
Sempre all'interno del registro il Titolare o suo Delegato, dovrà inoltre indicare (v. Art. 35 comma 11) se ritiene necessario prevedere un'attività di riesame (e con quale periodicità) per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati, almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.

107 Modalità di controllo

L'applicazione della procedura è monitorata mediante audit interni periodici condotti dal Titolare o suoi Delegati e dal DPO.

108 Strumenti Informativi coinvolti

a. Strumento "PIA" (CNIL) per la raccolta delle informazioni durante il processo DPIA o evoluzione dello stesso;
b. Software per la gestione del Registro dei Trattamenti;
c. Software di analisi dei rischi in ambito sicurezza delle informazioni (conforme agli standard ISO31000, ISO27001 e ISO27005);
d. Software di gestione degli Asset e relative Misure di Sicurezze;
e. Software di gestione del Dossier Data Protection.
f. Modalità di pubblicazione delle DPIA al fine di rendere trasparente l'azione del Titolare

Allegato L

Formulazione Contratti, Convenzioni Linee Guida

1 Scopo del Documento

Il presente documento ha l'obiettivo di fornire le istruzioni per una corretta elaborazione di bandi di gara, contratti e convenzioni relativi ad erogazione di servizi, al fine di garantire la conformità dei contenuti dei predetti documenti alle prescrizioni di cui al Reg. UE n. 679/2016 in materia di protezione dei dati personali (nel prosieguo richiamato con l'acronimo GDPR).
Le presenti linee guida rispondono all'esigenza di:

a. fornire indicazioni al Dirigente di riferimento per la predisposizione della descrizione del servizio da appaltare, tali da garantire l'immediata e chiara individuazione delle attività oggetto di appalto e di eventuali aspetti rilevanti ai sensi del GDPR;
b. individuare – in caso il servizio comporti attività soggette all'applicazione di quanto disposto dal GDPR - apposite "sezioni"/clausole da inserire nei bandi, contratti, convenzioni e che dovranno costituire elementi essenziali degli stessi;
c. consentire, successivamente, all'Ufficio Contratti di verificare che l'oggetto di gara sia chiaramente espresso e che il dirigente abbia provveduto ad indicare nei contenuti da inserire nel bando e nel contratto gli elementi necessari ai fini del GDPR;
d. fornire le corrispondenti indicazioni nel caso di convenzioni/protocolli di intesa che non prevedono per loro natura una procedura di gara.

2 Premessa

Le Linee Guida descritte in questo documento si applicano in ipotesi di redazione di disciplinari di gara, contratti e convenzioni aventi ad oggetto la fornitura di servizi a Regione Toscana da parte di appaltatori.
Nel momento in cui un Dirigente di Regione Toscana predispone un nuovo bando per la fornitura di servizi, il contratto successivo all'aggiudicazione dello stesso o una convenzione è, dunque, tenuto ad applicare le indicazioni riportate nel presente documento.
Le linee guida vogliono essere, inoltre, strumento utile per l'Ufficio Contratti e l'Ufficio Legale di Regione Toscana, che potranno verificare la presenza nello specifico bando, contratto o convenzione esaminato/a, di tutti gli elementi necessari per la sua corretta stesura ai sensi del GDPR.

3 Contesto di riferimento

Le prescrizioni delle presenti Linee Guida sono predisposte in riferimento a categorie in cui sono classificate le diverse tipologie di servizi da appaltare.
Le categorie sono state definite in relazione alle specificità rilevanti di ognuna rispetto alle altre in riferimento ai contenuti che – ai sensi di quanto previsto dal GDPR – si deve prevedere di esplicitare nel bando, contratto o convenzione da predisporre per l'appalto del servizio richiesto.
Per ogni categoria sono stati individuati i servizi richiesti - oggetto del bando, contratto o convenzione da predisporre – che possono essere ricompresi nella categoria stessa, in quanto implicano aspetti uguali o analoghi da considerare e disciplinare ai fini del GDPR.

Infine, per favorire la classificazione del servizio richiesto nella categoria corrispondente sono stati anche rilevati i principali elementi distintivi, cioè quegli elementi caratteristici della categoria che la differenziano dalle altre.

Di seguito sono indicate le principali categorie, per ogni categoria è indicata una breve descrizione, i principali servizi che possono essere ricompresi a titolo esemplificativo, nonché i fattori che distinguono il tipo di contratto in merito alle prescrizioni GDPR.
Il ragionamento generale secondo il quale si procede ad attribuire il ruolo GDPR ai contraenti è il seguente:

1) Individuare in prima istanza i trattamenti/ servizi oggetto del contratto/ convenzione e chiedersi se questi prevedono il trattamento di dati personali oppure no
2) Nel caso che li preveda, quale sia il soggetto fra i contraenti che, per norma, è quello titolato alla loro gestione,
3) Se Il trattamento/servizio nella titolarità di uno dei soggetti vien svolto sulla base del contratto/convenzione da un altro, lo stesso contratto configura un rapporto fra titolare e Responsabile. Il Titolare (controller) è colui che per norma deve erogare quel servizio e decidere finalità e mezzi del trattamento connesso, mentre il Responsabile (Processor) è il soggetto che materialmente eroga o concorre ad erogare il servizio, senza entrare nel processo decisionale (su finalità e mezzi).
4) Se ognuno dei soggetti svolge quel servizio nell'ambito della propria Titolarità, determinando dunque autonomamente finalità e mezzi del trattamento, si configura un rapporto fra titolari autonomi
5) Se i soggetti concorrono anche con modalità differenti alle stesse finalità e concordano e individuano congiuntamente i mezzi, questo configura un rapporto fra titolari in regime di Contitolarità.
6) Se il contratto/convenzione non prevede esplicitamente riferimenti al trattamento di dati personali occorre chiedersi se l'attività per l'erogazione di servizi, che non prevedono trattamenti di dati personali, costituiscano comunque un rischio (rischio di interferenza) per la diffusione, accesso, distruzione di dati personali.
    a) In caso positivo occorre inserire nel contratto delle prescrizioni che consentano di ridurre il rischio di interferenza e sanzionare comportamenti che possano trasformare il rischio in effetti dannosi per gli interessati.
    b) In caso negativo, il rapporto giuridico non avrà impatti in materia di tutela dei dati personali e, pertanto, non saranno previste clausole DP.

Nel caso di contratti di acquisizione di servizi, risulta molto probabile che il rapporto che si va a prefigurare fra il soggetto che appalta il servizio e il soggetto esecutore del servizio sia del tipo Titolare/Responsabile; fanno eccezioni quei casi per cui il soggetto esecutore esplica quel servizio in virtù di norme (di legge, regolamentari o di qualsiasi altro tipo e da qualsiasi fonte, europea, nazionale o regionale) e processi di certificazione nazionali/europee che lo qualifichino come Titolare autonomo per quel servizio.
In questo caso il rapporto che si viene ad istaurare è fra Titolari Autonomi. Esempi possono essere il servizio di postalizzazione, il rilascio di credenziali di identità personale, taluni servizi professionali.

Dirette conseguenze del rapporto di titolarità autonoma risiedono:

a. nell'autonomia sanzionatoria, nel senso che il soggetto esecutore del servizio ne risponde direttamente, per norma;

b. nella non esistenza di potere di controllo tra titolari, contrariamente all'obbligo di verifica nei rapporti tra responsabile e titolare (in capo a quest'ultimo);
c. nell'assenza di specifico DPA nei casi in cui il rapporto di titolarità sia definito per legge.

Altra casistica da tenere presente è nel caso di contratti/convenzioni nell'ambito del quale i servizi che si vanno a contrattualizzare sono di utilizzo di competenze professionali, che esercitano la loro attività attraverso regole, e strumenti sotto l'esclusivo controllo dell'appaltatore. Anche in questo caso il rapporto che si viene ad instaurare è fra Titolari autonomi, e l'appaltatore provvederà ad autorizzare il personale, acquisito attraverso il contratto, ad eseguire i trattamenti di propria competenza su propri strumenti e secondo le misure di sicurezza da esso determinate.

Sulla base di tali considerazioni sono state individuate le seguenti categorie e i relativi Data Protection Agreement da mettere in atto :

Categoria	Descr. Categoria	Servizi compresi nella categoria	Elementi distintivi ai fini del GDPR	*DPA*
1	Utilizzo di risorse umane, applicazioni e sistemi del contraente	Servizi SaaS, Servizi Tesoreria, Conservazione a norma Servizi che hanno una loro specifica regolazione	Continuità del servizio, disponibilità del dato, evitare situazioni lock in	***Titolare/ responsabile*** ***Titolari autonomi***
2	Utilizzo sistemi IT e SW di base del contraente	Servizi IaaS	continuità del servizio, individuazione dei trattamenti IT	***Titolare/ responsabile (solo per i servizi di gestione IT)*** ***Titolari autonomi per specifici servizi (es. posta elettronica, SPID, portali amministrativi in rete)***
3	Servizio nel quale deve essere prevista la distruzione dei supporti magnetici e non, contenenti dati personali	Rottamazione HW, gestione archivi di deposito	Garanzie sulla distruzione del supporto fisico, modalità di esecuzione (la distruzione del supporto fisico non significa distruzione del dato che può continuare ad essere presente in altri supporti)	***Titolare/ responsabile***

Categoria	Descr. Categoria	Servizi compresi nella categoria	Elementi distintivi ai fini del GDPR	*DPA*
4	Servizi con uso prevalente di risorse umane che utilizzano per lo svolgimento delle proprie attività strumenti e mezzi di loro proprietà	Servizi di assistenza tecnica su finanziamenti europei, servizi di help desk, portierato, consulenza, progettazione, vigilanza, somministrazione di lavoro, servizi di sorveglianza sanitaria, servizi di orientamento e formazione lavoratori in difficoltà, servizi di formazione del personale dell'ente, servizio di gestione sinistri – assistenza	In questo caso l'elemento prevalente è l'utilizzo di risorse umane che svolgono il servizio, altrimenti si ricadrebbe nella categoria 1. La categoria 4 si distingue dalla 5 in quanto le attività appaltate sono svolte con mezzi e strumenti di proprietà della ditta aggiudicatrice e non dell'ente. Per l'aggiudicatrice va valutata la nomina a responsabile (prevista anche per la 5). Saranno differenti tra 4 e 5 le prescrizioni su misure di sicurezza.	***Titolare/ responsabile*** ***Per i servizi legati all'esercizio di professioni regolate per legge, il rapporto è, di norma, fra Titolari autonomi (es. servizi assicurativi, medico competente)***
5	Servizi con uso prevalente di risorse umane che utilizzano per lo svolgimento delle proprie attività strumenti e mezzi dell'ente	Servizi di assistenza tecnica su finanziamenti europei, servizi di help desk, portierato, stage, consulenza, progettazione, vigilanza, somministrazione di lavoro, produzione reportistica su conformità servizio Trio web learning, servizi per l'impiego e delle politiche attive	Qualora il soggetto contraente non abbia alcun controllo sulle modalità ed esecuzione delle attività di trattamento in quanto regolato da altre norme Nel caso in cui si configuri una autonomia nei mezzi e negli strumenti in uso dal contraente	***Il rapporto è fra titolari autonomi e il committente procede ad autorizzare il personale esterno.*** ***Titolare/ responsabile***

Categoria	**Descr. Categoria**	**Servizi compresi nella categoria**	**Elementi distintivi ai fini del GDPR**	***DPA***
6	Servizi in relazione a progetti di interesse regionale cofinanziati/finanziati dalla Regione	contratti/convenzioni con soggetti terzi che svolgono servizi sul territorio con finanziamento/cofinanziamento regionale	In questo caso si configura un rapporto fra titolari ed in capo a Regione Toscana rimane il monitoraggio dei trattamenti effettuati.	***Titolarità autonoma***
7	Servizi nell'ambito dei mezzi di comunicazione di massa in rete e social	monitoraggio dei mezzi di comunicazione di massa in rete,	Se i servizi hanno ad oggetto soltanto dati pubblici non comportano trattamenti, Nel caso in cui per l'esercizio di tali attività fossero coinvolti dati personali dell'appaltatore Se esistessero rischi di diffusione o accesso indebito a dati personali debbono essere previste specifiche prescrizioni	***Nulla*** ***Titolare/ Responsabile*** ***Prescrizioni***

Categoria	Descr. Categoria	Servizi compresi nella categoria	Elementi distintivi ai fini del GDPR	*DPA*
8	Servizi di assistenza, manutenzione e sviluppo HW e SW	Assistenza e manutenzione software e Hw, sviluppo, software	Si tratta di fornitura di servizi in ambito informatico (assistenza, manutenzione e sviluppo sw e hw), che non prevedono trattamenti di dati personali ma che potrebbero potenzialmente comportare accesso a dati personali da parte dell'esecutore . E' importante quindi chiarire bene nell'oggetto, come si svolge l'attività e, se in concreto potrà verificarsi un continuativo non occasionale accesso a contenitori di dati, in questo caso sarà necessario un rapporto titolare responsabile	***Prescrizioni*** ***Titolare Responsabile***
9	Servizi nei quali l'attività appaltata è prettamente artigianale/manuale e l'utilizzo di mezzi e strumenti informatici non è prevalente	Servizio mensa bar, manutenzione edifici ed impianti, pulizie, logistica,	Si tratta di attività che per loro natura non comportano trattamento di dati. Tuttavia in alcuni casi (es. nel servizio pulizie, se il soggetto consulta dati erroneamente lasciati sulle scrivanie) potrebbe esservi un coinvolgimento dell'aggiudicatrice e del suo personale in trattamenti, per cui devono essere indicate prescrizioni specifiche per tali ipotesi.	***Rapporto fra titolari autonomi qualora siano coinvolti non in maniera occasionale dati personali*** ***Prescrizioni negli altri casi***

Categoria	Descr. Categoria	Servizi compresi nella categoria	Elementi distintivi ai fini del GDPR	*DPA*
10	Servizi che vengono erogati congiuntamente fra più soggetti condividendo e individuando in modo congiunto le finalità, i mezzi e gli strumenti	Sistema di prenotazioni fra aziende sanitarie diverse utilizzanti un unico sistema informativo Nota: in questo caso si configura un rapporto fra titolari e se il servizio è dato in gestione ad un terzo, si configura un rapporto fra i Contitolari e il Responsabile. Nel rapporto di contitolarità può essere identificato il soggetto titolare che terrà i rapporti contrattuali e di altro tipo con Il responsabile	Di norma questa tipologia non si riscontra in appalti di servizi ma diviene possibile in convenzioni fra soggetti diversi che congiuntamente, condividendo finalità e mezzi, offrono un servizio comune agli interessati e che pertanto li percepiscono come un soggetto unitario.	***In questo caso il rapporto fra i soggetti è di contitolarità***
11	Casi In cui l'aspetto del trattamento dati non sia previsto	servizio aereo con elicotteri di supporto al sistema regionale di prevenzione e lotta attiva agli incendi boschivi e di protezione civile,	Casi in cui l'aspetto del trattamento dei dati non rileva.	***Verificare se effettivamente non esistano rischi di accesso non strutturato a dati personali.*** ***Nel caso comunque fornire delle prescrizioni***

4 Fasi di attività per la predisposizione di disciplinari di gara, contratti e convenzioni

Al fine della individuazione delle diverse categorie di rapporti che il contratto o convenzione viene ad instaurare si seguono i seguenti passi fin dalla predisposizione del bando se necessario:

a) Descrizione del servizio richiesto
b) Identificazione dei diversi servizi oggetto dell'appalto,
c) Valutare se e quali servizi comportano l'applicazione del GDPR rilevando se vengono trattati dati personali,
d) analisi dei servizi e riconducibilità ad una categoria come da tabella precedente. È possibile che un contrato/convenzione riguardi più servizi e che questi si riferiscano a categorie diverse. pertanto potranno anche esserci più DPA per un contratto/convenzione.

Qualora al bando preveda la sottoscrizione di contratto o convenzione, sarà in questi che saranno inserite gli articoli che regoleranno i rispettivi ruoli e responsabilità in termini di data protection, nel caso che il bando non preveda la stipula di un atto susseguente (vedi ad esempio Finanziamenti su progetti) la DPA relativa dovrà essere presente nel bando e ne dovrà essere richiesta la compilazione e la firma da parte del contraente e l'invio congiuntamente all'offerta di servizi/progetto pena la non sua valutazione.
Vale la pena ricordare che il GDPR richiede obbligatoriamente la redazione e sottoscrizione di un accordo fra le parti nel caso di un rapporto che preveda lo scambio di dati personali e più in generale il loro trattamento.

A supporto della classificazione nella corrispondente categoria, si fa riferimento ai contenuti della tabella sopracitata. In particolare, gli elementi distintivi riportati per ogni categoria hanno l'obiettivo di:

a) guidare l'autore del documento nel definire le ipotesi in cui un servizio può essere collocato in più categorie;
b) favorire l'esplicitazione delle misure specifiche che dovranno necessariamente essere riportate nel documento finale.

Gli esempi riportati sono solo esemplificativi, durante l'applicazione del GDPR si provvederà a fornire altri esempi inserendo i nuovi contratti e relativi DPA.

In caso non fosse possibile ricondurlo ad alcuna delle categorie predeterminate o in ipotesi in cui il Dirigente abbia difficoltà nell'effettuare tale attività, è tenuto a rivolgersi immediatamente all'Ufficio del DPO.

4.1 Contenuti da esplicitare nel bando, nel contratto o nella convenzione

In caso si accerti che il servizio comporti attività rilevanti ai sensi di quanto disposto dal GDPR dovranno essere inseriti nel disciplinare di gara, contratto, convenzione, contenuti conformi alle prescrizioni corrispondenti nelle specifiche "sezioni" previste per quella determinata categoria contrattuale ("Prescrizioni per la descrizione del servizio e l'accertamento dell'ambito di applicazione del GDPR", "Prescrizioni comportamentali per le

risorse umane coinvolte", "Prescrizioni Data Protection per risorse organizzative", "Prescrizioni per le risorse tecnologiche – misure di sicurezza").

A tal fine le indicazioni sono declinate con riferimento ai seguenti aspetti:

a) qualificazione del rapporto con l'aggiudicatario in una delle figure GDPR;
b) indicazioni sui contenuti che devono essere esplicitati sia nel bando, che nel contratto che seguirà all'aggiudicazione;
c) Prescrizioni comportamentali per le risorse umane coinvolte;
d) Prescrizioni Data Protection per risorse organizzative;
e) Prescrizioni per le risorse tecnologiche – misure di sicurezza.

Tali regolazioni fanno parte dei contenuti dei diversi Data Protection Agreement di cui

1) ***DPA Titolare Responsabile-(sub responsabile) allegato D/E***
2) ***DPA Fra titolari autonomi, allegato C***
3) ***DPA di Contitolarità, allegato F***.

Nel caso dell'appalto di servizi, convenzioni o protocolli di intesa, nei quali non siano previsti trattamenti di dati personali, ma per i quali esiste un rischio di interferenza con trattamenti del Titolare o del Responsabile, il DPA deve prevedere prescrizioni e clausole che riducano il rischio di interferenza, e qualora si concretizzi lo sanzionino.

Per rischio di interferenza si intende l'occasionale accesso a dati personali da parte di persone non coinvolte nel relativo trattamento. Ueste sono persone che devono essere istruite affinché pur potendolo fare, non mettano in atto comportamenti che possano produrre Data Breach o incidenti di sicurezza.

Allegato M-N

Applicazione delle Misure di sicurezza

Linee Guida

1 Scopo del documento

Il presente documento ha lo scopo di fornire linee guida per l'applicazione ai contesti reali delle misure di sicurezza descritte ***nell'allegato B delle linee guida Data Protection by Design/Default***.

Questo vale sia per quei trattamenti per i quali viene prodotta una specifica DPIA ***(vedasi per questo l'allegato I alle linee guida Data Protection by Design/Default)*** sia per tutti gli altri trattamenti, in quanto per tutti deve essere riportata nel registro dei trattamenti l'informazione in merito alle misure di sicurezza adottate.

Le misure di sicurezza come descritto negli allegati citati, sono sia trasversali a tutti i dati e trattamenti nell'ambito di un definito contesto (data Center, fornitore, ecc..), sia specifici, cioè aggiuntivi per lo specifio Asset.

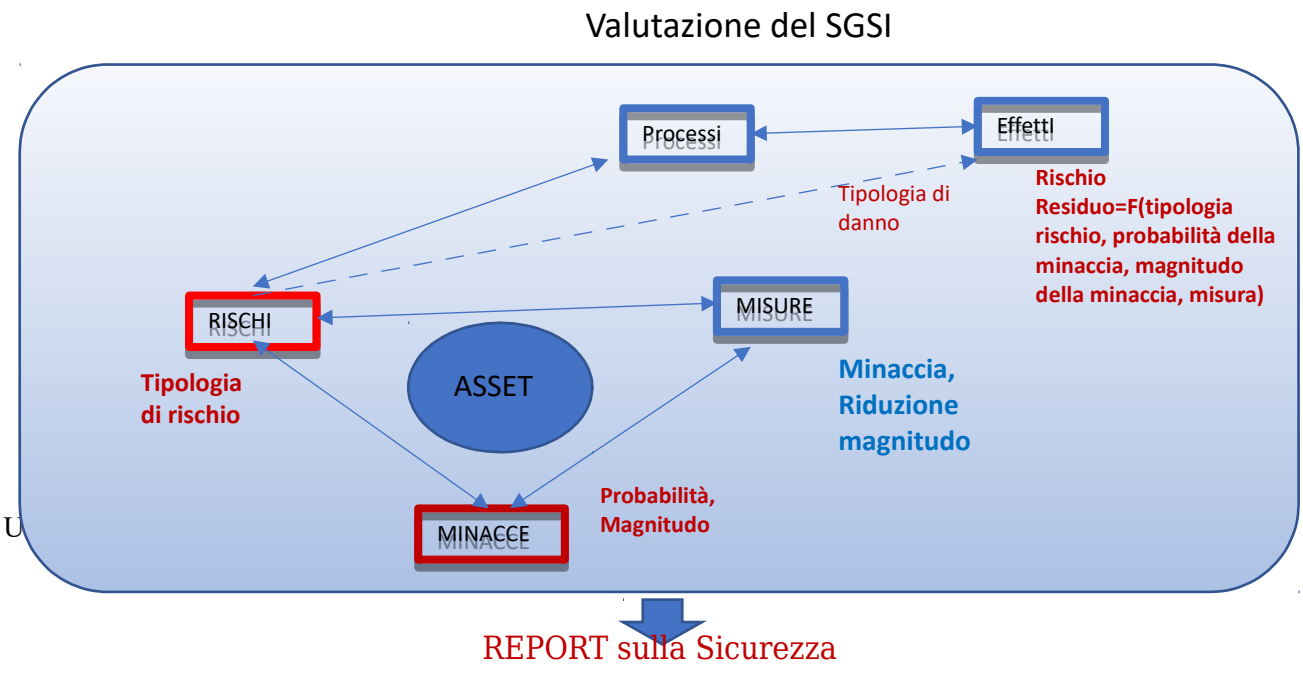
Si ricorda che per Asset, si intende l'elemento di un sistema di Asset che va a definire il contesto *(envirorment)* tecnico, organizzativo e tecnologico, che presiede ai trattamenti di dati ed in particolare di dati personali.
L'insieme degli asset: - sistemi elaborazione fisici, basi di dati, applicazioni, reti, locali fisici, ecc.. - costituisce l'ambiente, il sistema tecnologico entro il quale si attuano trattamenti, il loro livello di sicurezza dipende pertanto dalla sicurezza delle diverse componenti.

109 Premessa

Tutte le informazioni raccolte ed elaborate durante il processo di analisi dei rischi (sia in ambito Data Protection by Design/Default sia per una specifica DPIA) devono essere formalizzate a supporto della realizzazione del piano della sicurezza.

Tipicamente, all'interno di un processo di analisi dei rischi occorre almeno tracciare:

1. Dati e trattamenti da proteggere e relativi Asset (asset primari)
2. Valorizzazione delle vulnerabilità e minacce (Impatti e probabilità)
3. Contromisure di mitigazione del rischio
4. Valore del rischio residuo



Tutte queste informazioni concorrono a realizzare un piano di valutazione e trattamento del rischio che deve essere supportato dalle relative risorse (economiche, organizzative e tecniche) affinché il piano sia effettivamente realizzabile.

110 Valutazione delle contromisure di mitigazione dei rischi

Tutta la documentazione prodotta all'interno del processo di DPIA ma anche nell'ambito della progettazione di un nuovo sistema o revisione di uno esistente, partendo dal censimento e descrizione del trattamento, passando dalle valutazioni preliminari per arrivare, quando necessario, al calcolo di analisi dei rischi e relativo piano di trattamento, devono concorrere alla realizzazione di un Report finale in grado di dimostrare, oltre ovviamente ai risultati ottenuti, la corretta esecuzione formale del processo e la sua aderenza ai requisiti richiesti dal GDPR.
Costituiscono parte fondamentale di tale report finale la valutazione dell'adeguatezza e applicabilità delle contromisure di sicurezza.

Viene quindi richiesto al Security Manager, con l'ausilio degli Specialisti di Sicurezza e/o responsabile dei sistemi informativi e/o responsabile infrastrutture, di valutare l'adeguatezza delle misure di sicurezza di base per garantire *un'adeguata sicurezza*, ma al contempo per valutare le misure di sicurezza specifiche da adottarsi puntualmente per un determinato trattamento in base alle valutazioni emerse in fase di progettazione (design) oppure durante le valutazioni di Data Protection Impact Assessment.

111 Modello per la Valutazione delle contromisure di sicurezza

Al fine di censire correttamente le misure di sicurezza che concorrono alla sicurezza di un trattamento è stata predisposta un'apposita modulistica basata sulle contromisure di sicurezza in analogia con quanto necessario in fase di DPIA seppur più ridotte.
Le misure di sicurezza sono quindi da censirsi per ogni trattamento soggetto a DPIA o meno e da documentarsi attraverso l'apposita modulistica.
I dati richiesti si riferiscono ovviamente alla "Anagrafica del Trattamento" che riportiamo per chiarezza ma che già è stata predisposta al fine della registrazione del trattamento nell'apposito registro:

Gruppo	Campo	Descrizione
Quale è il trattamento in considerazione ?		

	Denominazione Trattamento	Indicare la denominazione del trattamento (da PIA)
	Finalità	Indicare la finalità del trattamento (da PIA)
	Utilizzo	Indicare l'utilizzo che ne viene fatto del trattamento (da PIA)
Quali sono le responsabilità connesse al trattamento?		
	Titolare del trattamento :	Indicare il riferimento del titolare del trattamento (da PIA)
	Responsabile del trattamento	Indicare l'eventuale Responsabile del trattamento quando presente (da PIA)
Ci sono standard applicabili al trattamento?		
	Standard applicabili	Indicare se il trattamento è soggetto a standard applicabili (da PIA))
Valutazione delle misure di sicurezza		
	Valutatore delle misure di sicurezza	Indicare il nominativo di colui che ha compilato la valutazione delle contromisure di sicurezza
	Approvatore della valutazione	Indicare il nominativo di colui che ha approvato la compilazione delle contromisure di sicurezza

Nel folder ***"Contromisure adottate"*** viene richiesto al compilatore di valutare per lo specifico trattamento ogni singola contromisura applicata secondo il seguente schema:

Campo della tabella	Descrizione del campo
Descrizione del combinato fra rischio e minaccia	Descrizione del rischio, della minaccia o categorie di minacce, e i probabili effetti dannosi sugli interessati
Cod. contromisura	E' un codice alfanumerico che identifica univocamente la contromisura
Classe contromisura	Le contromisure secondo lo schema dell'applicativo PIA sono suddivise in 3 classi distinte: *Misure applicate ai dati* *Misure generali di sicurezza dei sistemi*

	Misure Organizzative
Contromisura di sicurezza	Descrizione sintetica della contromisura di sicurezza
Descrizione della contromisura	Descrizione estesa della contromisura di sicurezza
Modalità di applicazione della contromisura in RT	Descrizione delle modalità con cui la contromisura è stata applicata in Regione Toscana
Livello di maturità	Livello di maturità raggiunto per la contromisura di sicurezza secondo lo schema riportato in tabella “Legenda Maturity Level”
Descrizione del livello di maturità	Descrizione (automatica) riportata in base al livello di maturità raggiunto
Misura Generale o specifica	Indicare se la misura di cui beneficia il trattamento è una misura generale del SGSI o una misura specifica valutata in corso di DPIA/Progettazione
Adeguatezza della contromisura al trattamento	Indicare se il livello di efficacia della contromisura è considerato adeguato per lo specifico trattamento. I valori di questo campo possono essere : *SI* *NO* *RIVEDERE*

Al fine di rendere agevole il lavoro di attribuzione di misure di sicurezza adeguate ad ogni trattamento occorre come più volte specificato, un catalogo dei contesti tecnici organizzativi, degli asset che li costituiscono e per ognuno di questi l’associazione alle misure di sicurezza, anch’esse contenute in un apposito catalogo, adottate in modo trasversale a quel specifico contesto. A quelle trasversali comuni a tutti i trattamenti si aggiungeranno quelle specifiche sulla base della valutazione del rischio residuo e del danno potenziale.
A seguire si riporta la legenda dei livelli di maturità applicabili all’interno del campo “Livello di maturità” per ogni contromisura valutata.

112 Legenda Maturity Level

Livello di maturità		Descrizione
0	Inesistente	Completa assenza di qualsiasi processo consapevole. L'organizzazione non si è ancora resa conto che c'è un problema che va affrontato. Il controllo di sicurezza non è attivo
1	Iniziale	Vi sono indicazioni che l'organizzazione si è resa conto dell'esistenza di problemi che devono essere affrontati. Tuttavia, invece di processi standardizzati ci sono approcci ad hoc che tendono ad essere applicati singolarmente o caso per caso. L'approccio generale alla gestione è disorganizzato. Mancanza completa di una policy e procedure per l'attivazione del controllo di sicurezza
2	Ripetibile	I processi sono sviluppati al punto che persone diverse impegnate nello stesso lavoro adottano procedure simili. Non c'è addestramento formalizzato né comunicazione di procedure standard e la responsabilità è lasciata al singolo. C'è un alto grado di fiducia sulle conoscenze dei singoli e pertanto gli errori sono probabili. Lo sviluppo del controllo di sicurezza è appena iniziato e il suo completamento richiederà un lavoro significativo per soddisfare i requisiti.
3	Definito	Le procedure sono state standardizzate, documentate, e comunicate mediante addestramento. E' comunque lasciata al singolo l'incombenza di seguire questi processi, ed è improbabile che le non conformità siano scoperte. Le procedure stesse non sono sofisticate ma consistono nella formalizzazione di prassi esistenti. Il controllo di sicurezza è in fase di implementazione ma non completato o implementato parzialmente.
4	Gestito	È possibile monitorare e misurare la conformità alle procedure ed effettuare azioni correttive dove i processi non appaiono funzionare efficacemente. I processi sono soggetti a costante miglioramento e assicurano buone prassi. L'automazione e la strumentazione sono usate in maniera limitata o frammentaria. Lo sviluppo del controllo di sicurezza è completo, il processo / controllo è stato implementato ed ha iniziato ad essere operativo
5	Ottimizzato	I processi sono stati affinati fino ad un livello di prassi ottimale, quale risultato di continui miglioramenti e del confronto col modello di maturità di altre aziende. Il requisito del controllo di sicurezza è pienamente soddisfatto, funziona completamente come previsto, viene attivamente monitorato e migliorato, e non vi sono evidenze sostanziali per gli auditors.

113 Strumenti Informativi coinvolti

- Catalogo degli ambienti tecnologici/organizzativi e relativi asset (da realizzare)
- Catalogo delle misure di sicurezza e loro collegamento con catalogo ambienti/asset
- Catalogo delle principali minacce
- Strumento "PIA" (CNIL) per la raccolta delle informazioni durante il processo DPIA, o suo evoluzione (raccomandata).
- Strumento software di analisi dei rischi in ambito sicurezza delle informazioni (conforme agli standard ISO31000, ISO27001 e ISO27005)

Allegato O

Dossier Data Protection

Linee guida per la sua formazione

1 Scopo del documento

Il presente documento descrive i contenuti del Dossier Data Protection quale contenitore documentale degli elementi costitutivi di un processo e del suo ciclo di vita.
Nasce pertanto con il primo atto che si riferisce ad un processo e si alimenta di tutta la documentazione che riguarda il ciclo di vita di quel processo.

114 Premessa

Il Dossier è costituito pertanto da tutti gli atti e i documenti che accompagnano un processo produttivo, dalla sua ideazione alla sua realizzazione e messa in esercizio. Al fine di rendere più chiaro questo concetto facciamo un esempio:
La Regione Toscana intende avviare sul territorio un servizio di assistenza agli anziani non autosufficienti (servizio badanti).

Procedimenti	**Riflessi sul Dossier D.P.**
La giunta approva una delibera che fornisce gli indirizzi, gli obiettivi, i vincoli, i criteri attraverso i quali realizzare il servizio Pronto Badanti	Viene aperto un Dossier, viene allegata la delibera e aggiunte informazioni di contesto quali eventuali atti precedenti, leggi di riferimento, le tipologie di dati che saranno trattati e le categorie degli interessati coinvolti, viene descritto il processo e i soggetti coinvolti, ecc..
Il settore competente predispone il progetto organizzativo e tecnico che approva con decreto e finanzia l'operazione	Il decreto e il progetto vengono registrati all'interno del Dossier, vengono confermate, integrate o variare le informazioni di contesto fornite precedentemente sulla base del progetto. Vengono individuati i soggetti da coinvolgere nella realizzazione del servizio individuando per ciascuno il sotto-processo a suo carico e vengono, ai diversi soggetti, attribuite le figure organizzative previste al GDPR
Il settore competente predispone il bando di gara attraverso il quale individuare i soggetti per i diversi sotto-processi, e le convenzioni con altri soggetti istituzionali e lo approva con decreto o più decreti. Nella stesura del bando e della convenzione si tiene conto delle specificità da inserirvi ai fini del GDPR sulla base delle relazioni che si vengono a creare in termini di Data Protection	Anche tali atti entrano a far parte del Dossier
Viene emesso il bando e stipulati i contratti, vengono stipulate le convenzioni	Anche questi documenti entrano a far parte del dossier
Prima dell'avvio del servizio viene valutato se occorre procedere alla	Nel dossier viene riportata la decisione presa e se è stata realizzata una DPIA anche il

realizzazione della DPIA	report finale viene riportato all'interno del Dossier
Se l'avvio del servizio prevede trattamenti in carico alla regione Toscana (titolare) si procede alla loro registrazione nel registro dei trattamenti	La registrazione dei trattamenti comporta il collegamento fra trattamenti e dossier
Qualora a seguito del perfezionamento dei contratti o delle convenzioni si addivenisse ad una modifica del progetto	La modifica del progetto già inserito nel dossier, entra a far parte del dossier stesso
Se nel corso di gestione del servizio accadessero degli incidenti Data Protection	La registrazione nel registro degli incidenti comporta la registrazione dell'incidente anche nel dossier

Come si vede il Dossier si forma naturalmente con il progredire degli atti e delle azioni, rappresenta pertanto un contenitore del sistema documentale dell'ente in cui confluiscono in modo diretto i documenti o i loro riferimenti e il suo scopo è quello di documentare quale sia stato il processo di messa in esercizio di servizi visti come insiemi di trattamenti a norma del GDPR.
L'attivazione e la gestione nel tempo del Dossier, non deve richiedere attività aggiuntive oltre a quelle già previste e pertanto potrà essere attivato quando la Regione disporrà di un sistema documentale e della interconnessione dello stesso con la procedura degli atti, con il registro dei trattamenti, con il registro degli incidenti. Allo stesso tempo è evidente che disporre del ***Dossier di Data Protection***, risulta determinate rispetto alla facilità di ricostruire l'albero delle decisioni e delle scelte in fase di analisi all'interno del processo di rendere conto (accountability) al garante, all'autorità giudiziaria, agli interessati.

115 Elementi costitutivi del Dossier Data Protection

Il dossier Data Protection è composto dalle seguenti sezioni e relativi dati.

115.1Sezione anagrafica

Contiene una sola istanza con i seguenti dati:

1) Nr. catalogo Dossier
2) Data apertura
3) Data Chiusura
4) Denominazione del processo
5) Descrizione sommaria del processo

115.2 Sezione istitutiva (1Istanza)

Contiene una sola istanza con i seguenti dati:

1) Riferimenti atto che ha dato luogo alla creazione del dossier
2) Riferimenti ad atti precedenti di cui quello istitutivo è conseguenza
3) Contesto normativo inteso come elencazione delle norme europee, nazionali , o regionali che inquadrano la liceità per il titolare nel perseguire quegli obiettivi attraverso la attivazione di processi e trattamenti dati
4) Data, Struttura competente e proponente l'atto

5) Tipologia di atto

115.3Sezione atti successivi

Contiene tante istanze quanti sono gli atti che si riferiscono al Processo con i seguenti dati:

1) Riferimenti atto
2) Data, Struttura competente e proponente l'atto
3) Tipologia di atto

115.4Sezione processo

Contiene tante istanze quante sono le versioni della sezione:

1) Descrizione testuale del processo
2) Descrizione tramite schema
3) Soggetti coinvolti e loro titolo di coinvolgimento

115.5Sezione dati

Contiene tante istanze quante sono le versioni della sezione:

1) Dati trattati
   a) Tipologia del dato (dati personali comuni, particolari, sanitari, giudiziari, ecc..
   b) Formato dei dati (immagini, testi, ….)
   c) Supporti (digitali, non digitali, …)
2) Interessati (le caratteristiche delle persone cui si riferiscono i dati personali)
   a) Categorie degli interessati (minori, disabili, ……)
   b) Numerosità egli interessati coinvolti (numero potenziale, riferimento geografico, ….)

115.6Sezione figure GDPR e relazioni

Contiene tante istanze quante sono le relazioni che si vengono a instaurare fra i soggetti:

1) Binomio Soggetto-Ruolo GDPR
2) Tipologia di relazione (Titolare-Titolare, Titolare-Responsabile[-sub responsabile], Contitolarità, …..)
3) Documento (DPA) Data Protection Agreement, tramite il quale i soggetti regolano le loro relazioni e relativi impegni GDPR

115.7Sezione Trattamenti

Contiene tante istanze quante sono i trattamenti che compongono il processo:

1) Riferimento registro trattamenti, denominazione trattamento
2)

115.8 Sezione DPIA

Contiene tante istanze quante sono le versioni della sezione:

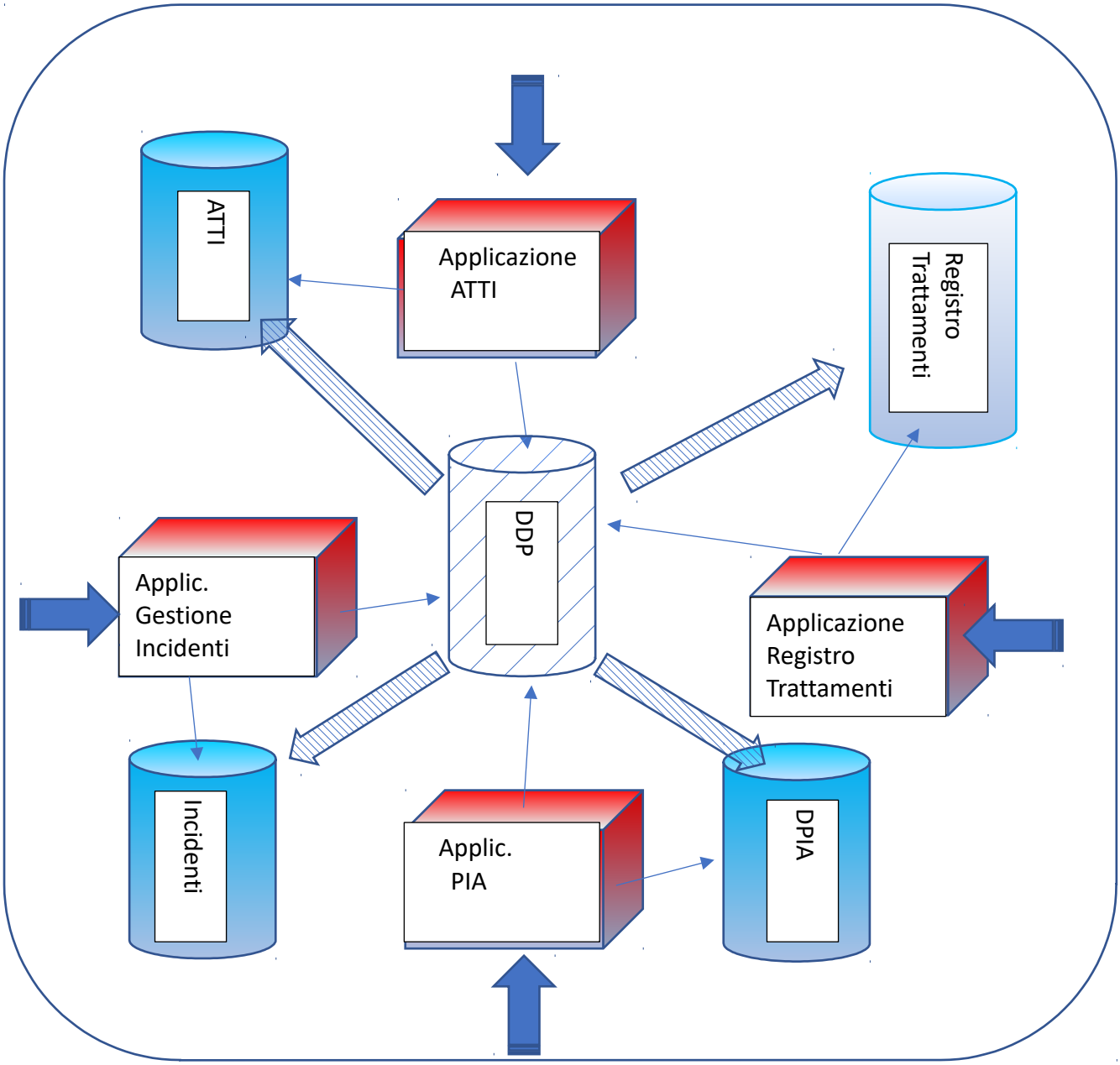
1) Report DPIA

116 Schema delle relazioni fra i contenuti informativi

Come rappresentato nello schema successivo, il Dossier Data Protection (DDP) viene alimentato automaticamente dalla:

a) procedura degli atti,
b) procedura di gestione dei trattamenti,
c) dalla procedura di gestione degli incidenti,
d) dalla procedura di DPIA.

117 Schema collegamento Dossier con altri archivi DP



Dallo schema si evince come il **Dossier Data Protection** costituisca un contenitore di meta dati che descrivono i vari oggetti e un insieme di riferimenti ad oggetti che sono registrati in altri repositori e come le operazioni di scrittura dei metadati nel DDP siano effettuate dalle procedure di gestione di quegli oggetti.
Pertanto il Dossier viene a formarsi automaticamente senza l'esigenza di operazioni aggiuntive.