ARPAT
Agenzia regionale
per la protezione ambientale
della Toscana

Decreto del Direttore generale nr. 186 del 31/12/2019

Proponente: Mario Daddi

SIRA

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

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

Responsabile del procedimento: *Marcello Mossa Verre*

Estensore: Mario Daddi

Oggetto: Disciplinare sull'utilizzo della posta elettronica, sull'accesso a internet, sull'utilizzo e la gestione degli strumenti e servizi relativi alle tecnologie dell'informazione e della comunicazione, sulle modalità per effettuare i trattamenti dati. Modello organizzativo per la data protection

ALLEGATI N.: 1

Denominazione	*Pubblicazione*	*Tipo Supporto*
Allegato A - Disciplinare ICT	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 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 – 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;

Visto il D. Lgs. 196 del 30/06/2003 (Codice privacy), integrato con le modifiche introdotte con D. Lgs. 101 del 10/08/2018, in adeguamento al GDPR;

Visto il Decreto del Direttore generale n. 171 del 28/12/2017 con il quale è stato approvato il "Disciplinare ICT e trattamenti dati - Revisione 01 (Disciplinare sull'utilizzo della posta elettronica, sull'accesso a internet, sull'utilizzo e la gestione degli strumenti e servizi relativi alle tecnologie dell'informazione e della comunicazione, sulle modalità per effettuare i trattamenti dati)" e la "Politica ICT e trattamenti dati - Revisione 00";

Vista la Data protection policy regionale, basata su due macro linee, una sull'adeguamento dell'organizzazione (messa in atto da Regione Toscana con Delibera n. 521 del 23.04.2019 della Direzione organizzazione e sistemi informativi), una sulla 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, collegato al piano della Giunta regionale dal quale deriva obiettivi, tempi e strumenti in toto o in parte, questo anche nella volontà congiunta di operare 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";

Considerato che il Piano operativo di adeguamento al GDPR di cui al DDG 81/2019 prevede l'aggiornamento del Disciplinare ICT e trattamenti dati – Revisione 01 (DDG 171/2017), con allineamento alla citata Data protection policy di Arpat, alle linee guida per l'attuazione dei processi di cui alla DGRT 7677/2019 e al Codice privacy modificato con D. Lgs. 101 del 10/08/2018;

Visto il Decreto DG n. 182 del 23/12/2019 che approva la Data protection policy di ARPAT;

Ritenuto di dover approvare l'aggiornamento del Disciplinare ICT e trattamenti dati per adeguamento al Codice privacy aggiornato con D. Lgs 101/2018 e allineamento alla Data protection policy di ARPAT;

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 il "Disciplinare ICT e trattamenti dati – Rev. 02 ("Disciplinare sull'utilizzo della posta elettronica, sull'accesso a internet, sull'utilizzo e la gestione degli strumenti e servizi relativi alle tecnologie dell'informazione e della comunicazione, sulle modalità per effettuare i trattamenti dati. Modello organizzativo per la data protection")", in Allegato "A";
2. di abrogare l'Allegato A al decreto del Diretttore generale n. 171 del 28 .12.2017 (Disciplinare ICT e trattamenti dati Rev. 01);
3. 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;
4. di dichiarare il presente decreto immediatamente eseguibile, al fine di consentire il progressivo adeguamento dell'organizzazione dell'Agenzia al GDPR, che dovrà avvenire prima possibile e comunque entro 12 mesi dall'adozione;

Il Direttore generale
Ing. Marcello Mossa Verre*

* "Documento informatico sottoscritto con firma digitale ai sensi del D.Lgs 82/2005. L'originale informatico è stato predisposto e conservato presso ARPAT in conformità alle regole tecniche di cui all'art. 71 del D.Lgs 82/2005. Nella copia analogica la sottoscrizione con firma autografa è sostituita dall'indicazione a stampa del nominativo del soggetto responsabile secondo le disposizioni di cui all'art. 3 del D.Lgs 39/1993."

Il Decreto è stato firmato elettronicamente da:

- Paola Querci , sostituto responsabile del settore Affari generali in data 30/12/2019
- Andrea Rossi , responsabile del settore Bilancio e Contabilità in data 30/12/2019
- Marco Chini , il proponente in data 30/12/2019
- Paola Querci , Direttore amministrativo in data 30/12/2019
- Guido Spinelli , Direttore tecnico in data 30/12/2019
- Marcello Mossa Verre , Direttore generale in data 31/12/2019

ARPAT - DIREZIONE TECNICA - Settore Sistema Informativo Regionale Ambientale

Via Porpora, 22 - 50144 - Firenze

27/12/2019

ALLEGATO A

Disciplinare ICT e trattamenti dati

Revisione 02

Disciplinare sull'utilizzo della posta elettronica, sull'accesso a internet, sull'utilizzo e la gestione degli strumenti e servizi relativi alle tecnologie dell'informazione e della comunicazione, sulle modalità per effettuare i trattamenti dati. Modello organizzativo per la data protection

Estensore: Ing. Mario Daddi

Proponente: Dott. Marco Chini

Approvazione: Ing. Marcello Mossa Verre

tel. 055.32061 - fax 055.3206324 - p.iva 04686190481 - www.arpat.toscana.it

per comunicazioni ufficiali PEC: arpat.protocollo@postacert.toscana.it - (accetta solo PEC),
per informazioni ambientali: 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

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

Articolo 1
Finalità e ambito di applicazione

Il Titolare, con l’approvazione del presente Disciplinare, mette in atto le misure tecniche e organizzative per garantire, ed essere in grado di dimostrare, che il trattamento dei dati è effettuato in modo conforme alla normativa vigente.

Il presente documento disciplina l'utilizzo, la gestione, la pianificazione e il controllo delle attività che riguardano le tecnologie dell'informazione e della comunicazione (ICT) e i trattamenti dati effettuati dal personale dipendente dell'Agenzia e da tutti gli altri soggetti che a vario titolo prestano servizio o attività per conto e nelle strutture di ARPAT.

Il Disciplinare viene redatto per le seguenti principali finalità:

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

1. adottare un unico riferimento normativo per comunicare con estrema chiarezza ai lavoratori e ai Responsabili:
    - le corrette modalità per l'utilizzo degli strumenti ICT aziendali loro assegnati;
    - la modalità di effettuazione dei trattamenti dati.
2. attuare le principali disposizioni previste dalla legislazione vigente in materia di tecnologie dell'informazione e della comunicazione e data protection e, in particolare:
    - attuare gli adempimenti previsti dal Regolamento (UE) 679/2016, noto come GDPR, relativi alla protezione dei dati, tra cui adempimenti del Titolare (art. 24), protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (art. 25), definizione dei compiti dei Responsabili dei trattamenti (art. 28), tenuta del Registro Trattamenti (art. 30), adozione di misure di sicurezza adeguate al rischio (art. 32), notifiche delle violazioni di dati personali all'autorità di controllo e agli interessati (articoli 33 e 34), valutazione d'impatto sulla protezione dei dati e consultazione preventiva (articoli 35 e 36), diritti degli interessati (CAPO III del GDPR);
    - attuare, nei casi in cui non vengono trattati dati personali, misure di sicurezza corrispondenti a quelle previste dal GDPR, al fine di garantire adeguato livello di tutela dei dati e delle informazioni trattate e unicità di gestione;
    - adempiere a quanto prescritto dal Garante per la Protezione dei dati personali nel provvedimento a carattere generale del 01/03/2007 in materia di posta elettronica e accesso a Internet, attraverso la definizione di regole comuni per tutelare i reciproci diritti e doveri di lavoratori e datore di lavoro, la sicurezza dei dati e la privacy;
    - ridurre la probabilità che comportamenti, anche inconsapevoli, possano innescare problemi o minacce alla riservatezza, integrità e disponibilità dei dati;
    - rafforzare il ruolo dei servizi di posta elettronica, del sito web e della intranet dell'Agenzia, quali strumenti di comunicazione aziendale di uso generale su cui basare il conseguimento degli obiettivi di efficienza, efficacia, economicità, semplificazione;
    - rafforzare e favorire l'impiego di tecnologie e software *open source*;
    - rafforzare e favorire il riuso, l'accesso e la fruibilità dei dati e documenti di cui è titolare ARPAT;
3. definire il diritto dell'Amministrazione di verificare che le risorse ICT vengano utilizzate correttamente, che non si verifichino usi impropri e individuare le modalità con cui l'Amministrazione esercita tale diritto di verifica;
4. definire il diritto di lavoratori (e di terzi) a una sfera di riservatezza anche nelle relazioni lavorative.

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

Le prescrizioni contenute si aggiungono e integrano le norme già previste dal contratto collettivo nazionale di lavoro, dalla normativa in materia di protezione dei dati personali e tecnologie ICT e dalla documentazione di sistema vigente in ARPAT.

Articolo 2
Definizioni e abbreviazioni

Amministratori di sistema: sono figure professionali critiche per i trattamenti dati in quanto operano in un contesto ove possono tecnicamente accedere, anche in modo fortuito, a dati personali o riservati e sono, in molti casi, concretamente “responsabili” di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione degli stessi dati. Ad essi si applicano le disposizioni di cui all'art. 9 del presente Disciplinare.

Autorizzati (incaricati): si tratta delle persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare, dal Delegato o dal Responsabile (denominati “incaricati” nella precedente normativa). Rientra in questa categoria tutto il personale dell'Agenzia e tutti gli altri soggetti che a vario titolo prestano servizio o attività per conto e nelle strutture di ARPAT (ai sensi dell’art .2-quaterdecies, comma 1, D. Lgs. 196/2003).

Codice privacy: Decreto legislativo 30 giugno 2003, n. 196, modificato con decreto legislativo 10 agosto 2018, n. 101.

Codice dell'amministrazione digitale (CAD): Decreto legislativo 7 marzo 2005, n. 82, modificato e integrato con Decreto legislativo 22 agosto 2016 n. 179 e poi con Decreto legislativo 13 dicembre 2017 n. 217;

Data Protection Officer (DPO): acronimo inglese del Responsabile della Protezione dei Dati (vedi Responsabile della Protezione dei Dati o RPD).

Data Security Officer (DSO): acronimo inglese del Responsabile della sicurezza IT (vedi Responsabile della sicurezza 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.

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 immagine facciale o i dati dattiloscopici (art. 4 GDPR).

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

Dati genetici: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione (art. 4 GDPR).

Dati giudiziari (dati relativi a condanne penali e reati - art. 10 GDPR): i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale (art. 4 D. Lgs. 196/2003).

Dati particolari (art. 9 GDPR): dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale della persona.

Dati personali: dato personale è qualunque informazione relativa a 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 uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (art. 4 GDPR).

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 (art. 4 GDPR).

Datore di lavoro: il soggetto titolare del rapporto di lavoro con il lavoratore ai sensi dell'art. 2 del D.Lgs. 81/2008.

Delegato: si tratta del soggetto delegato dal Titolare al trattamento di dati personali (ai sensi dell'art. .2-quaterdecies, comma 1, D. Lgs. 196/2003 "Attribuzione di funzioni e compiti a soggetti designati") e delegato al trattamento di altre tipologie di dati.

I Delegati sono il direttore tecnico, il direttore amministrativo e i responsabili delle partizioni organizzative previste nell'Atto di organizzazione.

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.

Dossier data protection: è il dossier in cui viene raccolta la documentazione che attesta il rispetto degli obblighi del Titolare di cui all'art. 24 del GDPR, di cui si riporta estratto: "il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere

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

in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento". Il Dossier data protection contiene pertanto tutte quelle analisi e valutazioni che vengono fatte al momento della emissione di qualunque atto che comporti, come conseguenza, il trattamento di dati personali. Il Dossier data protection è gestito dall'Ufficio DPO.

DPIA: è l'acronimo di Data Protection Impact Assessment (vedi "Valutazione di impatto sulla protezione dei dati", nel seguito).

GDPR: è l'acronimo di General Data Protection Regulation, con cui si identifica il Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali, entrato in vigore il 25 maggio 2018, con applicabilità diretta in tutti gli Stati membri.

ICT: Tecnologie dell'Informazione e della Comunicazione (Information Communication Technology). Comprende tutto ciò che riguarda i servizi informatici (quali ad esempio la posta elettronica, l'accesso a Internet, la condivisione delle risorse, ecc.), i sistemi applicativi (quali ad esempio il sistema di protocollo informatico, i sistemi gestionali, la intranet, il sito web istituzionale, ecc.), le postazioni di lavoro, la telefonia, le reti dati, le apparecchiature per le funzioni di stampa / fotocopia / scansione / fax, ecc.

Incaricati: vedi Autorizzati.

Lavoratori: persone che prestano il proprio lavoro alle dipendenze di un datore di lavoro, secondo la definizione di cui all'art. 2 del D. Lgs. 81/2008. Rientra in questa categoria tutto il personale dell'Agenzia e i tutti gli altri soggetti che a vario titolo prestano servizio o attività nelle strutture di ARPAT.

Politica per l'ICT e i trattamenti dati: descrive la Politica per l'ICT e i trattamenti dati di ARPAT in coerenza con la normativa di settore (Codice dell'Amministrazione digitale, Codice Privacy e altra normativa nazionale e regionale).

Processi GDPR: si tratta dei 4 macro processi, individuati nella "Data protection policy" di ARPAT, necessari a giungere alla piena attuazione del GDPR: Data Protection by design / by default (che include la gestione del Registro Trattamenti e delle DPIA), Garanzia e tutela dei diritti degli interessati, Gestione degli incidenti e violazioni, Accountability.

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 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.

Registro Trattamenti: registro delle attività di trattamento svolte sotto la responsabilità del Titolare. Contiene le informazioni indicate nell'art. 30 del GDPR. Il Registro è tenuto in forma scritta e anche in formato elettronico e, su richiesta, è messo a disposizione dell'autorità di controllo. ARPAT utilizza un unico registro per tutte le attività di trattamento svolte al suo interno.

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

Regolamento regionale sul trattamento dei dati sensibili e giudiziari: si tratta del regolamento regionale sul trattamento dei dati sensibili e giudiziari da parte della Regione Toscana, aziende sanitarie, enti, aziende e agenzie regionali e soggetti pubblici nei confronti dei quali la Regione esercita poteri di indirizzo e controllo", di cui al Decreto n. 6/R del 12/2/2013 del Presidente della Giunta Regionale (ed eventuali successive modificazioni).

Identifica i tipi di dati sensibili e giudiziari trattati e descrive, per queste tipologie di dati, le finalità e le operazioni eseguibili.

É emesso in attuazione dell'articolo 1, comma 1, della legge regionale 3 aprile 2006 n. 13, redatto a sua volta in applicazione dell'art. 22 del Codice Privacy "Principi applicabili al trattamento di dati sensibili e giudiziari" (ridefiniti, nel GDPR, come dati particolari e dati relativi a condanne penali e reati).

Referenti ICT: nell'ambito degli autorizzati vengono individuate le figure professionali critiche per il funzionamento del sistema ICT di ARPAT, denominate "Referenti ICT", i quali sono preposti alla gestione del ciclo di vita di specifiche componenti tecnologiche o funzioni in qualità di titolare o di collaboratore.

Nell'ambito dei Referenti ICT vengono individuate le figure professionali critiche per i trattamenti dati, denominate "amministratori di sistema".

L'elenco dei Referenti ICT e degli amministratori di sistema è mantenuto aggiornato sulla intranet di Agenzia.

Relazione sull'ICT: si tratta di un documento soggetto ad aggiornamento annuale, che il Titolare approva prima della predisposizione del bilancio (esercizio e investimento), dei piani di attività, del piano di formazione e del piano della qualità, su proposta del Responsabile ICT.

Contiene quanto segue:

- Descrizione dei servizi erogati e SLA garantiti;
- Criticità connesse alla sicurezza ICT e misure adottabili per la loro risoluzione;
- Necessità che riguardano le infrastrutture di supporto (rete dati, energia elettrica, condizionamento, ecc.);
- Analisi della coerenza tra l'organizzazione e l'utilizzo dell'ICT (nell'ottica di promuovere iniziative di cooperazione alla revisione della organizzazione dell'Agenzia, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrativa).

Responsabile del trattamento dati (di seguito anche solo Responsabile): si tratta del soggetto preposto dal Titolare al trattamento di dati personali ai sensi dell'art. 28 del GDPR (in inglese "processor").

Responsabile della protezione dei dati (RPD o DPO): è designato dal Titolare ai sensi dell'art. 37 del GDPR, in funzione delle qualità professionali, in particolare della conoscenza

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

specialistica della normativa e della prassi in materia di protezione di dati e della capacità di assolvere i compiti cui è preposto, specificati all'art. 39 del citato Regolamento:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR, nonché da altre disposizioni dell'Unione o dello Stato italiano relative alla protezione dei dati;

b) sorvegliare l'osservanza del GDPR, di altre disposizioni dell'Unione o dello Stato italiano 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;

d) cooperare con l'autorità di controllo;

e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva nei casi che richiedono una valutazione d'impatto sulla protezione dei dati, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Può essere un dipendente del Titolare o assolvere i suoi compiti in base a un contratto di servizi.

I suoi dati di contatto sono pubblicati dal Titolare e comunicati all'autorità di controllo.

Non riceve alcuna istruzione relativa all'esercizio dei suoi compiti. Non è rimosso o penalizzato dal Titolare o dai Responsabili dei trattamenti per l'adempimento dei propri compiti. Riferisce direttamente al Titolare. E' tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione e dello Stato Italiano. Può svolgere altri compiti e funzioni purché non diano adito a un conflitto di interessi.

Responsabile ICT: è il Responsabile dell'organizzazione, l'innovazione e le tecnologie ICT (**Responsabile della transizione al digitale o RTD**), individuata in Allegato 1. E' in possesso dei requisiti previsti per tale incarico dall'art.17 del Codice dell'amministrazione digitale. Ha le responsabilità che le leggi vigenti attribuiscono alla figura del responsabile dei sistemi informativi e i compiti indicati all'art. 17 del Codice dell'amministrazione digitale.

Responsabile della sicurezza IT o DSO (Data Security Officer) o Security IT manager: figura implicitamente prevista dal GDPR per supportare il Titolare nei suoi compiti di supervisione e controllo delle misure di sicurezza adottate, per determinare la loro adeguatezza nel tempo e per garantire il rispetto del principio di separazione tra chi le misure le deve attuare (il Responsabile ICT) e chi invece deve controllarle (Responsabile della sicurezza IT).

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

Scheda sistema: scheda che descrive il tipo di trattamento effettuato con un sistema applicativo o, più in generale, con un sistema ICT. La scheda contiene le principali informazioni che possono interessare gli utilizzatori del servizio o del software, quali ad esempio la descrizione del sistema e delle principali tipologie di dati trattati, i criteri su cui si basa l'organizzazione e la gestione del sistema cui si riferisce, le categorie di persone che possono accedere ai dati gestiti, le eventuali regole di utilizzo, informazioni sui backup e sulle eventuali criticità.

L'elenco aggiornato delle “schede sistema” in vigore è consultabile in specifica sezione della intranet, dalla quale è possibile accedere alle stesse schede.

Scheda gestione: scheda che contiene le informazioni riservate al personale addetto all'amministrazione, gestione o manutenzione di un sistema ICT.

L'elenco aggiornato delle “schede gestione” in vigore è consultabile in specifica sezione della intranet, dal quale è possibile accedere alle stesse schede.

Security IT manager: vedi Responsabile della sicurezza IT.

Strumenti elettronici: elaboratori, programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento (la definizione è tratta dall'art. 4 del Codice Privacy). Dunque rientrano in questa categoria i personal computer, i notebook, i tablet, i cellulari, gli smartphone, ecc.

TIC: Tecnologie dell'informazione e della comunicazione (sigla italiana corrispondente al più noto acronimo inglese ICT, Information Communication Technology).

Titolare del trattamento dati dell'Agenzia art. 24 GDPR (C74-C78) (in inglese Controller) è ARPAT, rappresentato dal Direttore Generale. E’ 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).

Trattamento dati: qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.

La definizione include sia i trattamenti di dati personali, sia le altre tipologie di dati.

Ufficio DPO: il DPO, se nominato come soggetto esterno all’Agenzia, è supportato internamente da un ufficio, denominato Ufficio DPO. L’Ufficio DPO supporta il Titolare, i Delegati e gli autorizzati nella attuazione della normativa relativa alla protezione dei dati

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

personali. L'Ufficio DPO è una struttura prevista nella Data protection policy di ARPAT, derivante dall'esigenza di avere un punto di riferimento organizzativo interno per l'attuazione della normativa. Presso l'Ufficio DPO sono dislocati i "data protection specialist" sopra definiti, che hanno la funzione di supportare la Direzione e le strutture di ARPAT nella attuazione del GDPR.

Valutazione d'impatto sulla protezione dei dati: valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali, ai sensi dell'art. 35 del GDPR.

E' approvata dal Titolare, e predisposta dal Direttore competente (punto 9.3 della Data Protection Policy di ARPAT) prima di procedere al trattamento, 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.

Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

La valutazione è richiesta in particolare nei seguenti casi:

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;

b) il trattamento, su larga scala, di dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché 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;

c) il trattamento, su larga scala, di dati personali relativi a condanne penali e reati, di cui all'articolo 10 del GDPR;

d) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico;

e) specifiche tipologie di trattamento appositamente individuate e rese pubbliche dall'autorità di controllo.

Per l'effettuazione della valutazione il Titolare si consulta con il Responsabile della protezione dei dati ed è supportato dal Responsabile ICT.

Violazione dei dati personali: 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.

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

Articolo 3
Principali riferimenti normativi

I principi applicati nella stesura del presente Disciplinare sono tratti dal quadro normativo che segue:

1. Costituzione: articoli 15 (libertà e segretezza della corrispondenza), 97 (organizzazione dei pubblici uffici).
2. Codice civile: articoli 2087 (tutela delle conduzioni di lavoro), 2104 (diligenza del prestatore di lavoro), 2105 (obbligo di fedeltà) e 2106 (sanzioni disciplinari).
3. Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016, 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, noto come GDPR).
4. Codice in materia di protezione dei dati personali (D.Lgs. n. 196/2003, noto come Codice Privacy).
5. Codice dell'amministrazione digitale (D.Lgs. 7 marzo 2005 n. 82).
6. Decreto Legislativo 12 febbraio 1993, n. 39 (Norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche).
7. Decreto Legislativo 27 gennaio 2010, n. 32 (Attuazione della direttiva 2007/2/CE, che istituisce un'infrastruttura per l'informazione territoriale nella Comunità europea – INSPIRE).
8. D.Lgs. 9 aprile 2008, n. 81 (norme in materia di tutela della salute e della sicurezza nei luoghi di lavoro, con particolare riferimento alle disposizioni sulle attrezzature munite di videoterminali): 173, 174, allegato XXXIV.
9. L. 20 maggio 1970, n. 300 (Statuto dei lavoratori): 4 (impianti audiovisivi), 7 (sanzioni disciplinari), 8 (divieto di indagini sulle opinioni), 14 (diritto di attività sindacale).
10. Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (DPR 445/2000): articoli 14 (trasmissione del documento informatico), 17 (segretezza della corrispondenza telematica).
11. Codice di comportamento dei dipendenti pubblici (DPR 62/2013).
12. Legge 7 agosto 1990 n. 241 (aggiornata con le modifiche introdotte dalla l. 15/2005 e dalla l. 80/2005) Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi.
13. Disciplina delle attività di informazione e di comunicazione delle pubbliche amministrazioni (Legge 7 giugno 2000, n. 150).

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

14. Direttiva 27.11.2003 sull'impiego della posta elettronica nelle pubbliche amministrazioni della Presidenza del Consiglio dei Ministri – Dipartimento per l'innovazione e le tecnologie.
15. “Linee guida del Garante per posta elettronica e internet”, emanate con deliberazione 1 marzo 2007 n. 13.
16. Provvedimento del 27.11.2008 del Garante per la protezione dei dati personali “Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema” (pubblicato su G.U. n. 300 del 24.12.2008 e modificato in base al provvedimento del 25.06.2009).
17. Direttiva 2006/24/CE del Parlamento Europeo e del Consiglio del 15.03.06 riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione.
18. Linee guida nazionali per la valorizzazione del patrimonio informativo pubblico (anno 2014), allegato alla Determinazione Commissariale n. 95/2014 del 26-06-2014 dell'Agenzia per l'Italia Digitale.
19. Legge Regionale n. 54 del 5 ottobre 2009 (Istituzione del sistema informativo e del sistema statistico regionale. Misure per il coordinamento delle infrastrutture e dei servizi per lo sviluppo della società dell’informazione e della conoscenza).
20. Legge Regionale n. 30 del 22 giugno 2009 (Nuova disciplina dell'Agenzia regionale per la protezione ambientale della Toscana (ARPAT).
21. Vigente Atto di disciplina dell'organizzazione interna di ARPAT (abbreviato in “Atto di organizzazione”).
22. Vigente Regolamento in materia di procedimenti amministrativi, di supporto tecnico ed attività di controllo ambientale e del vigente Regolamento per l’esercizio del diritto di accesso ai documenti amministrativi, diffusione ed accesso alle informazioni ambientali, accesso civico semplice e generalizzato.
23. Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015: “Misure minime di sicurezza ICT per le pubbliche amministrazioni”.
24. “Disciplinare per l’utilizzo della posta elettronica e di internet per l’articolazione organizzativa della Giunta regionale”, di Regione Toscana, utilizzato come riferimento per alcuni articoli.
25. Circolare AGID 18 aprile 2017 n. 2/2017.
26. Data protection policy di ARPAT (Decreto DG n. 182 del 23/12/2019).

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

Articolo 4
Principi generali su cui si basa l'utilizzo delle risorse ICT e il trattamento dei dati aziendali

L'utilizzo delle risorse ICT messe a disposizione del personale si ispira ai principi di diligenza e correttezza, atteggiamenti richiesti nello svolgimento di ogni atto o comportamento posto in essere nell'ambito del rapporto di lavoro, in qualsiasi forma esso sia.

Le risorse ICT fornite da ARPAT si utilizzano unicamente per perseguire gli scopi lavorativi.

La protezione dei dati e delle informazioni nel loro complesso è condizione necessaria per salvaguardare il loro valore economico e garantire il rispetto dei requisiti di sicurezza che la normativa vigente impone a tutti i soggetti che, a vario titolo, effettuano il trattamento di dati personali e non.

ARPAT inoltre, deve assicurare la funzionalità e il corretto impiego degli strumenti informatici da parte dei lavoratori, anche per conseguire gli obiettivi di efficienza, efficacia ed economicità.

I trattamenti dati si ispirano ai principi che regolano la trasparenza, l'accountability, la partecipazione e l'efficacia dell'azione amministrativa e che disciplinano le attività di informazione e di comunicazione delle pubbliche amministrazioni.

La gestione del livello di riservatezza dei dati, documenti e informazioni è finalizzata da una parte ad assicurare un adeguato livello di protezione dei dati personali e di altri dati riservati (quali ad esempio informazioni che riguardano l'attività amministrativa e sanzionatoria), dall'altra a promuovere la diffusione di informazioni di interesse pubblico e risponde ai criteri definiti nella "Politica per l'ICT e i trattamenti dati".

I trattamenti di dati personali rispondono ai principi della normativa sulla privacy, di seguito riassunti:

1. **liceità, correttezza e trasparenza**: sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
2. **limitazione della finalità**: sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, effettuato in modo conforme al GDPR, non è considerato incompatibile con le finalità iniziali;
3. **minimizzazione dei dati**: sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
4. **esattezza**: sono esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;

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

5. **limitazione della conservazione**: sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatta salva l'attuazione di misure tecniche e organizzative adeguate, richieste dal GDPR a tutela dei diritti e delle libertà dell'interessato;
6. **integrità e riservatezza**: sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

Articolo 5
Titolarità degli strumenti, delle apparecchiature informatiche e dei dati

ARPAT è proprietaria degli strumenti e delle apparecchiature ICT assegnate ai dipendenti, ai collaboratori e a tutti gli altri soggetti che a vario titolo prestano servizio o attività per conto o nelle strutture di ARPAT. Tali strumenti sono affidati ai medesimi con l'obbligo di custodirli con cura, evitando manomissioni, danneggiamenti o utilizzi, anche da parte di altre persone, per scopi non consentiti.

Gli strumenti e le apparecchiature ICT sono restituite ad ARPAT alla cessazione dell'esigenza per la quale erano state previste, ad esempio alla cessazione dell'incarico, del rapporto di lavoro, del rapporto di collaborazione, del rapporto contrattuale con ARPAT o a seguito di trasferimento presso altra struttura di ARPAT.

ARPAT è titolare dei dati che vengono prodotti dai propri dipendenti, collaboratori e da tutti gli altri soggetti che a vario titolo prestano servizio o attività per conto e nelle strutture dell'Agenzia.

Articolo 6
Il software

ARPAT, nei limiti dell'efficienza operativa connessa con l'uso del software utilizzato, privilegia l'open source.

Il software sviluppato dal personale di ARPAT e da tutti gli altri soggetti che a vario titolo prestano servizio o attività per conto o nelle strutture di ARPAT è open source, distribuibile gratuitamente a terzi, con licenza GPL.

Articolo 7
Rispetto della proprietà intellettuale e delle licenze

Tutti gli autorizzati sono tenuti al rispetto delle leggi in materia di tutela della proprietà intellettuale e non possono, sulle apparecchiature fornite, installare hardware o software né

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

duplicare o utilizzare software che non sia stato preinstallato, installato, fornito o comunque autorizzato da ARPAT.

Articolo 8
Utilizzo dei dati

I dati e le informazioni sono beni di ARPAT.

I dati e le informazioni detenute su apparecchiature di ARPAT o altri supporti sono utilizzati dal personale, anche fuori dagli uffici di ARPAT, ai soli fini lavorativi.

Nessun dato di ARPAT o personale può essere trattato o memorizzato su dispositivi elettronici di qualsiasi tipologia, non finalizzati all'attività lavorativa.

ARPAT favorisce il riuso, l'accesso e la fruibilità dei dati e documenti di cui è titolare. Tali attività avvengono in modo controllato per assicurare il rispetto della normativa in materia di protezione dei dati personali e la riservatezza delle istruttorie.

I dati e i documenti che ARPAT pubblica, con qualsiasi modalità, senza l'espressa adozione di una licenza di uso, si intendono rilasciati come dati di tipo aperto ai sensi dell'art. 68, comma 3 del Codice dell'amministrazione digitale.

I dati e le informazioni memorizzate, elaborate e/o comunicate attraverso le apparecchiature informatiche in uso presso ARPAT possono essere oggetto di controllo da parte dell'Amministrazione per esigenze legate a motivi di sicurezza o controllo di spesa o efficienza e manutenzione dei servizi.

Articolo 9
Compiti e responsabilità

1. Modello organizzativo data protection

Il Titolare dei trattamenti dati con l'approvazione del presente Disciplinare designa i Delegati e gli Autorizzati ai trattamenti, definisce le modalità per effettuare i trattamenti dati (personali e non personali) e per assegnare i compiti agli autorizzati.

Il Direttore tecnico, il Direttore amministrativo e i responsabili delle partizioni organizzative di ARPAT vengono individuati quali Delegati.

Hanno le responsabilità e i compiti loro attribuiti dal regolamento organizzativo di ARPAT e, inoltre, espletano i compiti assegnati nel seguito del presente articolo.

I Responsabili sono le persone fisiche o giuridiche, le autorità pubbliche, i servizi o altri organismi esterni che trattano dati personali per conto del Titolare a seguito di nomina formale. I loro compiti sono disciplinati da un contratto o altro atto giuridico stipulato con il Titolare.

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

Gli Autorizzati (o incaricati) sono le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare, dal Delegato o dal Responsabile.

Rientra in questa categoria tutto il personale dell'Agenzia e tutti gli altri soggetti che a vario titolo prestano servizio o attività per conto e nelle strutture di ARPAT sotto il controllo del Titolare, di un Delegato o di un Responsabile (ai sensi dell'art .2-quaterdecies, comma 1, D. Lgs. 196/2003).

Con l'approvazione del presente Disciplinare tutti i dipendenti di ARPAT assumono il ruolo di Autorizzati.

2. Compiti del Responsabile ICT

E' Responsabile dell'organizzazione, l'innovazione e le tecnologie ICT, con i compiti indicati all'art. 17 del Codice dell'amministrazione digitale.

Coordina le attività che riguardano l'ICT e promuove la realizzazione di un sistema integrato per la compliance alle diverse normative (ICT, GDPR, archivio, processi, procedimenti, ecc.).

Supporta il Titolare, i Delegati e gli autorizzati nella attuazione delle misure di sicurezza previste dalle disposizioni contenute nel Codice dell'Amministrazione Digitale, Codice Privacy, e altra normativa di settore.

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché dell'oggetto, del contesto e delle finalità del trattamento, come anche dei rischi di varia probabilità e gravità sui diritti e le libertà delle persone fisiche, sulla riservatezza, integrità e disponibilità dei dati, sulla continuità operativa, propone la messa in atto di misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

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 di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali 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.

Nel valutare l'adeguato livello di sicurezza, tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

A tal fine:

1. Predispone e tiene aggiornati il Disciplinare ICT e trattamenti dati e la Politica per l'ICT e i trattamenti dati in accordo con le disposizioni contenute nella normativa di settore.

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

2. Predispone annualmente la Relazione sull'ICT per l'approvazione del Titolare prima della definizione dei piani annuali.
3. Predispone, tiene aggiornato e pubblica sulla intranet un elenco dei servizi erogati con informazioni sulla struttura di riferimento per l'utilizzo, sulla struttura responsabile del sistema, sui livelli di servizio garantiti, sui Referenti ICT e amministratori di sistema preposti.
4. Garantisce la disponibilità e la corretta attuazione di procedure aggiornate per il backup, la custodia di copie di sicurezza e per il ripristino della disponibilità dei dati e dei sistemi.
5. Effettua la nomina individuale degli amministratori di sistema stabilendo per ciascuno di essi l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato, su un documento interno che mantiene aggiornato, consultabile sulla intranet e disponibile in caso di accertamenti, anche da parte del Garante.
6. Coordina le attività e verifica con cadenza almeno annuale l'operato degli amministratori di sistema.
7. Predispone e aggiorna le procedure relative alla gestione delle tecnologie dell'informazione e della comunicazione.
8. Assicura, nello svolgimento delle sue attività, che la protezione dei dati personali avvenga fin dalla progettazione e per impostazione predefinita.
9. Predispone sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte di amministratori di sistema (salvo i sistemi che effettuano trattamenti per fini esclusivamente amministrativo-contabili). Le registrazioni (access log) hanno caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni comprendono i riferimenti temporali e la descrizione dell'evento che le ha generate e sono conservate per un congruo periodo, non inferiore a sei mesi.
10. Supporta il Titolare nella valutazione d'impatto dei trattamenti sulla protezione dei dati.
11. In caso di violazione di dati personali informa il Titolare e il Responsabile della sicurezza IT (DSO o Security IT manager) senza ingiustificato ritardo dopo esserne venuto a conoscenza. Documenta e registra le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Supporta il Titolare nella notifica della violazione all'autorità di controllo (da fare entro 72 ore nei casi in cui la violazione presenti un rischio per i diritti e le libertà delle persone fisiche).

Il Responsabile ICT, con riferimento ai suoi compiti, risponde,direttamente al Titolare.

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

3. Compiti del Titolare

Mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che i trattamenti sono effettuati conformemente al GDPR. A tal fine:

1. Designa il Responsabile ICT.
2. Approva la Politica per l'ICT e i trattamenti dati.
3. Approva il Disciplinare ICT e trattamenti dati.
4. Approva il Registro Trattamenti.
5. Approva la DPIA.
6. Approva l'informativa.
7. Designa il Responsabile della protezione dei dati, pubblica i suoi dati di contatto e li comunica all'autorità di controllo.
8. Designa il Responsabile della sicurezza IT (DSO) e il Responsabile dell'Ufficio DPO.
9. Definisce le misure per assicurare la costante attuazione del GDPR, regolamentando a tal fine la gestione dei **4 processi GDPR** individuati nella "Data protection policy" di ARPAT:
    a) **Data Protection by design / by default** (obblighi del Titolare di cui all'art. 25 del GDPR), ove hanno particolare rilevanza la gestione del Registro Trattamenti (art. 30 GDPR), la Valutazione d'impatto sulla protezione dei dati (DPIA, art. 35 GDPR);
    b) **Garanzia e tutela dei diritti degli interessati** (adempimenti previsti al capo III del GDPR, da art. 12 ad art. 23);
    c) **Gestione degli incidenti e violazioni** (obblighi del Titolare di cui all'art. 33 del GDPR);
    d) **Accountability** (obblighi del Titolare di cui all'art. 24 del GDPR);
10. Assicura che i compiti assegnati ai Responsabili siano disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri.
11. Approva la Relazione sull'ICT prima dell'approvazione dei piani annuali.
12. Approva le procedure relative alla gestione delle tecnologie dell'informazione e della comunicazione.

4. Compiti assegnati al Responsabile della protezione dei dati (DPO)

1. Informa e fornisce consulenza al Titolare, ai Responsabili e agli autorizzati in merito agli obblighi derivanti dal GDPR, dal Codice Privacy e da altre disposizioni normative relative alla protezione dei dati.

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

2. Sorveglia l'osservanza del GDPR, del Codice Privacy e di altre disposizioni normative relative alla protezione dei dati, nonché delle politiche del Titolare 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 attività di controllo.
3. Fornisce, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e ne sorveglia lo svolgimento.
4. Coopera con il Garante per la protezione dei dati personali.
5. Funge 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 effettua, se del caso, consultazioni relativamente a qualunque altra questione.
6. Funge 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.

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.

5. Compiti assegnati all'Ufficio DPO

L'Ufficio DPO è previsto nel caso sia nominato, quale DPO, un soggetto esterno all'Agenzia.

L'Ufficio DPO supporta il Titolare, i Delegati e gli autorizzati nella attuazione della normativa relativa alla protezione dei dati personali. Propone un piano di azioni per la piena applicazione del GDPR ed è:

a) punto di riferimento multidisciplinare a supporto del Titolare, del DPO, dei Delegati e degli autorizzati;
b) punto di contatto con gli interessati;
c) punto di riferimento organizzativo di supporto alle interlocuzioni con il Garante;
d) punto di riferimento organizzativo per la gestione e la conservazione del Dossier data protection (vedi art. 10).

In caso di violazione di dati personali informa il Titolare e il Responsabile della sicurezza IT (DSO o Security IT manager) senza ingiustificato ritardo dopo esserne venuto a conoscenza. Documenta e registra le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Supporta il Titolare nella notifica della violazione all'autorità di controllo (da fare entro 72 ore nei casi in cui la violazione presenti un rischio per i diritti e le libertà delle persone fisiche), d'intesa con il Responsabile ICT.

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

6. Compiti assegnati al Responsabile della sicurezza IT (DSO o Security IT manager)

1. Governa la qualità nella sicurezza IT delle informazioni attraverso funzioni di monitoraggio, controllo delle misure applicate e indicazioni di miglioramento ai soggetti gestori e responsabili della sicurezza IT, verificandone l'applicazione e i relativi tempi.
2. Gestisce il processo di raccolta, gestione e analisi degli incidenti fra cui anche il processo di Data Breach previsto dal GDPR.
3. Supporta il Titolare negli adempimenti di cui all'art. 33 del GDPR (notifica di una violazione dei dati personali all'autorità di controllo).
4. Gestisce la documentazione relativa alle misure di sicurezza adottate nei diversi settori (infrastrutture, sistemi applicazioni), ai controlli effettuati, alle risultanze di tali controlli, ai disciplinari di utilizzo degli strumenti e servizi IT, rendendola immediatamente disponibile in caso di valutazioni, da parte del Garante, del livello di sicurezza adottato.
5. Predispone un piano annuale di interventi finalizzati a svolgere i compiti assegnati.
6. Collabora con il Responsabile della protezione dei dati (DPO/RPD) nelle valutazioni dei rischi e degli incidenti.
7. Collabora con il Responsabile del protocollo e degli archivi al fine dell'individuazione dei rischi e delle soluzioni per ridurli;
8. Collabora con il Responsabile ICT al fine dell'individuazione, programmazione e verifica dei progetti di "trasformazione digitale" in relazione all'obiettivo di innalzare il livello di sicurezza.

7. Compiti assegnati ai Direttori

Ai direttori sono delegate, per i trattamenti su cui hanno competenza di indirizzo e regolamentazione come da Registro Trattamenti, 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).

   Il Registro Trattamenti e la DPIA sono approvati dal Titolare.

8. Compiti assegnati a tutti i Delegati

Espletano i compiti istituzionali della partizione organizzativa che coordinano, nel rispetto delle Disposizioni generali, valide per tutti i trattamenti dati, contenute nel presente Disciplinare, nella

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

Politica per l'ICT e i trattamenti dati e successive disposizioni applicative e delle seguenti disposizioni specifiche.

Assicurano che i trattamenti di loro competenza si svolgano secondo le modalità indicate all'art.10 "Modalità per effettuare i trattamenti dati".

Definiscono gli ambiti di trattamento degli autorizzati mediante:

1. assegnazione formale delle attività e degli obiettivi;
2. definizione dei profili di autorizzazione del personale interno ed esterno che svolge attività per conto della struttura che coordinano. A tal fine:
   a) effettuano le richieste di abilitazione alle applicazioni mediante apposita modulistica;
   b) verificano periodicamente, e comunque almeno annualmente, la sussistenza delle condizioni per la conservazione dei profili di autorizzazione del personale interno ed esterno che svolge attività per conto della struttura che coordinano;
   c) assicurano che l'ambito di trattamento assegnato ai singoli autorizzati sia coerente ai compiti loro assegnati tenendo anche conto dei principi di adeguatezza, proporzionalità e necessità.

Assicurano il rispetto delle disposizioni del GDPR e Codice Privacy che si applicano alle specifiche attività istituzionali della struttura che coordinano.

Assicurano che il personale che svolge attività per conto della struttura che coordinano:

- si sia impegnato alla riservatezza o abbia un adeguato obbligo legale di riservatezza;
- si attenga alle misure di sicurezza indicate nell'Allegato 2 "Norme generali di comportamento prescritte agli autorizzati".

Assicurano la formazione di base dei propri collaboratori interni ed esterni in materia di sicurezza informatica e data protection (la formazione è effettuata al momento dell'ingresso dei collaboratori presso la struttura, nonché in occasione dei cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento dei dati).

Assicurano la presenza di procedure e regole di utilizzo per la gestione di eventuali strumenti informatici dei quali hanno il completo controllo diretto o la gestione applicativa.

Prescrivono adeguate misure di sicurezza aggiuntive qualora ritengano che le misure indicate nel Disciplinare non siano sufficienti a trattare la tipologia dei dati personali e delle informazioni gestite dalla propria struttura;

Partecipano al processo di pianificazione delle attività ICT segnalando le necessità informatiche della struttura che coordinano.

Mettono a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto dei loro obblighi e contribuiscono alle attività di revisione, comprese le ispezioni, realizzate dal Titolare (o da altro soggetto da questi incaricato).

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

Informano immediatamente il Titolare qualora ritengano che un'istruzione violi la normativa sulla privacy.

Vigilano sul rispetto delle disposizioni contenute nel presente Disciplinare e collaborano alla attuazione delle misure indicate.

9. Compiti aggiuntivi assegnati ai Delegati

Ad alcuni Delegati, individuati in Allegato 1, sono assegnati specifici compiti aggiuntivi necessari ad assicurare adeguato livello di tutela dei dati e delle informazioni trattate in ARPAT. Tali compiti sono mirati principalmente ad assicurare:

- il controllo sugli atti, al fine di assicurare che la protezione dei dati avviene fin dalla progettazione e per impostazione predefinita e l'accountability;
- la continuità di funzionamento delle infrastrutture di supporto (rete dati, energia elettrica, condizionamento, sistemi antincendio, servizi di videosorveglianza);
- la protezione delle aree e dei locali;
- la sicurezza nella gestione operativa dei beni ICT;
- la protezione degli apparati critici (server, router, ecc.);
- la protezione dei cablaggi critici (dorsali della rete dati, cavi di alimentazione degli apparati critici);
- lo svolgimento di alcune attività critiche relative alla gestione delle risorse umane (note informative ai nuovi autorizzati; note informative su assunzioni, cessazioni, trasferimenti, nomine Responsabili di struttura; formazione in materia di sicurezza informatica e privacy e rendicontazione).

10. Compiti assegnati ai Responsabili (art. 28 GDPR)

I Responsabili presentano 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 sono 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;

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

f) nonché a tutti gli altri elementi indicizzati all'art. 28, comma 3, GDPR;

g) definendo in modo chiaro quali siano gli obblighi e i diritti del Titolare e quali quelli del Responsabile, tendo nel debito conto l'attività di controllo propria del Titolare.

11. Compiti assegnati agli Autorizzati

I dipendenti ARPAT svolgono le attività loro assegnate nel rispetto delle norme generali di comportamento riportate in Allegato 2.

Il personale esterno si attiene alle istruzioni del preposto Responsabile, nel rispetto di quanto indicato all'art. 10 paragrafo "Trattamenti e servizi in outsourcing o in contitolarietà.

12. Compiti dei Referenti ICT

Nell'ambito degli autorizzati sono individuati i Referenti ICT, figure professionali critiche per il funzionamento dei sistemi ICT.

I Referenti ICT curano la gestione del ciclo di vita di specifiche componenti tecnologiche o funzioni in qualità di titolare o di collaboratore (gestione, controllo della configurazione e documentazione dei sistemi/funzioni a cui sono assegnati).

13. Disposizioni relative ad amministratori di sistema

Nell'ambito dei Referenti ICT sono individuati gli amministratori di sistema, figure professionali critiche per il funzionamento dei sistemi ICT e per i trattamenti dati, per i quali valgono le disposizioni aggiuntive riportate nel seguito.

Con la definizione di "amministratore di sistema" si individuano sia le figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti (che è la definizione che viene comunemente data in ambito informatico di amministratore di sistema), sia gli amministratori di database, gli amministratori di rete, gli amministratori di apparati di sicurezza, gli amministratori di sistemi software complessi.

Gli amministratori di sistema sono figure professionali critiche per i trattamenti dati in quanto:

- operano in un contesto ove possono tecnicamente accedere, anche in modo fortuito, a dati personali o riservati sebbene non siano preposti ordinariamente a operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni);
- sono, in molti casi, concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione degli stessi dati.

L'individuazione dei soggetti idonei a svolgere le mansioni di amministratore di sistema riveste una notevole importanza, costituendo una delle scelte fondamentali che, unitamente a quelle

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

relative alle tecnologie, contribuiscono a incrementare la complessiva sicurezza dei trattamenti svolti, e va perciò curata in modo particolare evitando incauti affidamenti.

Anche nei casi in cui le funzioni di amministratore di sistema sono attribuite solo nel quadro di una designazione quale “incaricato” del trattamento, il Titolare e il Delegato devono comunque attenersi a criteri di valutazione equipollenti a quelli richiesti per la designazione dei “Responsabili”.

La rilevanza, la specificità e la particolare criticità del ruolo di amministratore di sistema sono state considerate anche dal legislatore il quale ha individuato, con diversa denominazione, particolari funzioni tecniche che, se svolte da chi commette un determinato reato, integrano ad esempio una circostanza aggravante. Ci si riferisce, in particolare, all'abuso della qualità di operatore di sistema prevista dal codice penale per le fattispecie di accesso abusivo a sistema informatico o telematico (art. 615 ter) e di frode informatica (art. 640 ter) nonché per le fattispecie di danneggiamento di informazioni, dati e programmi informatici (articoli 635 bis e ter) e di danneggiamento di sistemi informatici e telematici (articoli 635 quater e quinques).

La designazione quale amministratore di sistema è individuale e reca l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

L'attribuzione di funzioni di amministratore di sistema avviene previa valutazione dell'esperienza, della capacità e dell'affidabilità dei soggetti designati, i quali devono fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza.

Articolo 10
Modalità per effettuare i trattamenti dati

1. Generalità

In Agenzia sono effettuati e consentiti i soli trattamenti dati che riguardano l'espletamento dei compiti istituzionali di ARPAT, i quali sono elencati nel Registro Trattamenti ed esplicitati, per ciascuna struttura, nell'Atto di organizzazione.

I trattamenti sono effettuati secondo i principi e le regole indicate nel presente Disciplinare, con uso di personal computer e altri dispositivi connessi in rete.

La protezione dei dati avviene fin dalla progettazione e per impostazione predefinita.

L’attivazione di trattamenti con nuovi sistemi informatici e/o tecnologie richiede il parere del Responsabile ICT/Ufficio DPO.

Per tutti i trattamenti è predisposta una informativa, pubblicata sul sito web, da richiamare in ogni forma di comunicazione con gli interessati.

Nel caso di raccolte sistematiche di dati personali tematici si forniscono agli interessati informative più specifiche.

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

Per tutti i trattamenti che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche si effettua la valutazione d'impatto sulla protezione dei dati (DPIA).

Per ogni processo data protection si costituisce un "dossier data protection" che tenga traccia delle scelte, delle misure e delle motivazioni che hanno portato alla loro determinazione. La DPIA, se effettuata, è conservata nel dossier.

Tutto il personale, nell'ambito delle proprie competenze, organizza e gestisce le attività assegnate in modo da assicurare il rispetto della normativa su:

- diritti degli interessati;
- misure di sicurezza;
- dossier data protection: notificare i decreti e gli eventuali altri atti di competenza, rilevanti per la data protection, all'Ufficio DPO per conservazione nel dossier;
- obblighi di comunicazione tempestiva delle violazioni di dati personali e degli attacchi informatici accertati o presunti, secondo le modalità indicate nella intranet.
- dati particolari e giudiziari;
- uso degli strumenti ICT e norme generali di comportamento in Allegato 2;
- trattamenti e servizi in outsourcing o in contitolarietà;
- accessibilità ai diversamente abili;
- formazione degli autorizzati.

Le suddette modalità sono approfondite nel seguito del presente articolo.

2. Registro Trattamenti (art. 30 del GDPR)

L'art. 30 del GDPR (C82) pone in capo al Titolare la responsabilità di tenere un registro delle attività di trattamento.

In ARPAT sono consentiti esclusivamente quei trattamenti dati riportati nel Registro Trattamenti, per le categorie di interessati e di dati personali in esso previste. Eventuali deroghe richiedono autorizzazione scritta del Titolare e contestuale aggiornamento del Registro.

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 le attività connesse.

b) di attribuire la responsabilità di promuovere l'aggiornamento del Registro ai Direttori, d'intesa con il Responsabile ICT e Ufficio DPO;

c) di attribuire ai Delegati (Direttori tecnico, amministrativo e Responsabili di struttura) i seguenti compiti e responsabilità:

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

i. **svolgere i soli trattamenti elencati nel Registro**;

ii. corredare i decreti di cui sono proponenti di tutti gli elementi e valutazioni relative alla data protection avvalendosi del supporto dell'Ufficio DPO, se necessario. A tal fine:

(a) indicare a quale trattamento è riconducibile l'atto tra quelli elencati nel Registro trattamenti;

(b) indicare se l'atto è rilevante ai fini della data protection, ovvero se rientra nelle categorie data protection sotto indicate;

(c) in caso affermativo indicare a quale **categoria di data protection** è riconducibile l'atto tra le seguenti:

- attivazione di trattamenti con nuovi sistemi informatici e/o tecnologie;
- affidamento di trattamenti dati a soggetti esterni con nomina di Responsabile (ad esempio contratti o accordi relativi ad attivazione di sistemi informatici o altre attività che prevedono trattamento dati, per i quali occorre prevedere, nell'atto, la nomina del Responsabile esterno come da art, 28 del GDPR e data protection policy);
- svolgimento di attività insieme a soggetti esterni con accordo di contitolarietà (ad esempio convenzioni, contratti o accordi con altri enti pubblici, per i quali occorre prevedere, nell'atto, l'accordo data protection di contitolarietà come da art. 26 del GDPR e data protection policy);
- normativa ICT e trattamenti dati, misure di sicurezza;
- Registro trattamenti;
- DPIA;

(c) prevedere, nel caso in cui l'atto appartenga a una delle categorie rilevanti per la data protection, l'impegno del proponente o del RUP, se diverso dal proponente, a notificare l'atto dopo l'approvazione all'Ufficio DPO per conservazione nel dossier data protection;

(d) allegare, nel caso in cui l'atto appartenga alla categoria data protection "attivazione di trattamenti con nuovi sistemi informatici e/o tecnologie" il parere del Responsabile ICT / Ufficio DPO che attesta la conformità alla normativa su data protection e ICT. Ai fini della conformità l'atto deve:

- includere l'informativa sul trattamento di cui all'art. 12 del GDPR o documentare le motivazioni per le quali non sia necessaria;
- includere 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;
- rispettare la normativa sull'ICT;

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

d) di attribuire all'ufficio che ha il compito istituzionale di effettuare il controllo formale sui decreti la responsabilità di verificare che gli atti proposti contengano gli elementi sopra elencati.

3. Deleghe nella gestione dei trattamenti

Le attività di trattamento sono delegate al Direttore tecnico, al Direttore amministrativo e ai Responsabili delle partizioni organizzative dell'Agenzia secondo le competenze definite nell'atto di organizzazione, nel presente Disciplinare ICT e puntualmente esplicitate nel Registro Trattamenti.

I Delegati, per svolgere i trattamenti, si avvalgono del personale assegnato alla struttura che coordinano (autorizzati), ai quali dovrà essere assicurata opportuna formazione.

I Delegati possono altresì avvalersi di servizi in outsourcing assicurando il rispetto, da parte del fornitore, delle modalità di trattamento previste nel presente Disciplinare.

4. Informative

ARPAT ha predisposto una "informativa privacy e trattamenti dati", consultabile online da parte di tutti gli interessati su http://www.arpat.toscana.it/utilita/privacy . Essa vale anche per i dipendenti ARPAT. Contiene le informazioni generali sulle modalità dei trattamenti dati, fornisce i dati di contatto del Titolare, del DPO, descrive i diritti degli interessati e le modalità per effettuare un reclamo all'autorità di controllo.

Tutto il personale è tenuto a:

- conoscerla;
- farvi riferimento in tutte le forme di comunicazione con l'esterno e l'interno (per ottemperare all'obbligo di far sapere agli interlocutori come vengono trattati i loro dati personali e quali siano i loro diritti);
- segnalare alla competente Direzione (generale, tecnica o amministrativa), tramite il Responsabile della struttura di assegnazione, eventuale necessità di aggiornamento;
- fornire agli interlocutori informative più specifiche nei casi in cui sia necessario attuare raccolte sistematiche di dati personali tematici non indicati nella informativa presente sul sito istituzionale.

L'aggiornamento della informativa è effettuato dal Titolare su proposta dei competenti direttori che, per questa attività, si avvalgono delle strutture competenti per i singoli trattamenti.

5. Data Protection Impact Assesment (DPIA)

Il GDPR all'art.35, in coerenza con il principio di sostanziale responsabilizzazione, prevede lo strumento della DPIA (Valutazione di impatto sulla protezione dei dati) quale processo mirato

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

alla valutazione dell'impatto del trattamento sulla protezione dei dati in funzione dei rischi e delle misure attivate per la loro riduzione.

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.

La DPIA è predisposta dai competenti direttori che, per questa attività, si avvalgono delle strutture di riferimento per quel trattamento e del supporto del Responsabile ICT/ Ufficio DPO. L'approvazione è a cura del Titolare, come da art. 35 GDPR.

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

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

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 GDPR oppure di dati relativi a condanne penali e a reati di cui all'art. 10 GDPR 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.

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 del GDPR richiede il parere degli interessati o dei loro rappresentanti.

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..

6. Dossier data protection

All'interno del Processo di Data Protection by design and by default (vedi obblighi del Titolare di cui all'art. 25 del GDPR), è prevista la costituzione di un dossier data protection per ogni processo, che tenga traccia delle scelte, delle misure e delle motivazioni che hanno portato alla loro determinazione.

Il dossier è tenuto aggiornato e conservato dall'Ufficio DPO con il contributo delle direzioni e strutture che hanno competenza sui trattamenti, che sono tenute a inviare all'Ufficio DPO tutti i documenti rilevanti ai fini della data protection.

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

Questo sia che sia stata effettuata a norma dell'art. 35 una specifica DPIA, sia che non sia stata effettuata in quanto ritenuta non necessaria.

Il dossier conterrà tutti 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.

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.

7. Diritti degli interessati (artt. 12-23 del GDPR)

Tutto il personale organizza le attività assegnate in modo da consentire e semplificare il rispetto dei diritti degli interessati e attuare, ciascuno nell'ambito delle proprie competenze, misure per:

1. minimizzare i dati trattati;
2. proteggerli da accessi non consentiti;
3. consentire e semplificare l'individuazione dei dati che afferiscono ai singoli interessati;
4. soddisfare le richieste degli interessati relative all'accesso ai dati che li riguardano;
5. rispettare i termini ultimi di cancellazione previsti dal Manuale di gestione del protocollo informatico, dei documenti e dell'archivio di ARPAT;
6. informare gli interessati sulle modalità di trattamento (fare riferimento alla specifica informativa applicabile).

A tal fine occorre istituire un "**fascicolo centralizzato del cittadino**", come collezione delle banche dati o archivi nelle quali sono presenti i relativi dati personali.

8. Sicurezza dei dati e comunicazione delle violazioni

Ciascun autorizzato, nell'ambito delle proprie competenze fornisce il proprio contributo e supporto al Titolare nel garantire la sicurezza dei dati e gli obblighi di cui agli articoli da 32 a 36 del GDPR, quali:

1. adozione di adeguate misure sicurezza;
2. comunicazione delle violazioni di dati personali e degli attacchi informatici accertati o presunti, secondo le modalità indicate nella intranet. La comunicazione è data senza ingiustificato ritardo dopo esserne venuti a conoscenza, corredata delle informazioni ad essa relativa (circostanze, conseguenze e azioni intraprese per porvi rimedio);
3. cooperazione con l'autorità di controllo, se richiesta;

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

4. contributo alla predisposizione della valutazione d'impatto sulla protezione dei dati e consultazione preventiva, se richiesto.

Il Titolare, con il supporto del DPO, Ufficio DPO e personale preposto al trattamento, valuta se dalla violazione derivino rischi per i diritti e le libertà degli interessati. In caso affermativo:

- notifica la violazione all'autorità di controllo senza ingiustificato ritardo e, ove possibile, entro 72 ore da quando ne è venuto a conoscenza (qualora la notifica non sia effettuata entro 72 ore, è corredata dei motivi del ritardo);
- comunica la violazione agli interessati senza ingiustificato ritardo.

9. Trattamenti di dati particolari e giudiziari

Per i trattamenti di dati personali particolari e giudiziari si applicano le ulteriori disposizioni regionali contenute nel regolamento regionale sul trattamento dei dati sensibili e giudiziari.

10. Strumenti utilizzati per i trattamenti e disposizioni sul loro uso

Per tutti i trattamenti sono utilizzati personal computer, altri dispositivi connessi in rete e strumenti di office automation.

Alcuni trattamenti sono effettuati con specifici sistemi ICT (ad esempio posta elettronica, condivisione delle risorse, intranet, sito istituzionale, sistema di protocollo informatico e gestione documentale, ecc.), che sono descritti in appositi moduli, denominati "schede sistema" e "schede gestione".

I principali elementi che costituiscono il sistema ICT di ARPAT sono descritti, nel loro insieme, nella Relazione sull'ICT e, in dettaglio, nelle Schede sistema e gestione, dei singoli applicativi e componenti tecnologiche, a cui si rimanda per ulteriori dettagli e specificità.

Le *schede sistema* sono destinate agli utilizzatori. Contengono per ciascun sistema le seguenti informazioni:

- una descrizione del sistema ICT e del trattamento effettuato (tipologie di dati trattati, principali caratteristiche del sistema, informazioni sui backup e sulle eventuali criticità);
- i criteri su cui si basa l'organizzazione, la gestione del sistema e l'accesso ai dati trattati;
- le registrazioni informatiche, ovvero i dati e i documenti prodotti dall'applicativo di cui è prevista la conservazione per legge o regolamento e i tempi di conservazione previsti;
- le eventuali regole di utilizzo.

Le *schede gestione* sono destinate ai tecnici manutentori, denominati "Referenti ICT". Contengono, per ciascun sistema, le informazioni necessarie ad assicurare interscambiabilità e continuità operativa, quali:

- le procedure di intervento che devono essere eseguite in caso di emergenza e tutte le informazioni che consentano a un tecnico informatico (e in alcuni casi anche a un non

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

informatico) che non conosce la configurazione del sistema specifico, di ripristinarne il funzionamento in caso di guasto;

- le informazioni necessarie a reperire rapidamente la documentazione applicabile e il software eventualmente occorrente a eseguire le procedure di intervento nei casi di emergenza;
- la descrizione delle attività che riguardano la amministrazione/gestione del sistema.

Le schede sistema e gestione sono poste sulla intranet per consultazione, insieme al loro elenco, avendo cura di proteggere le informazioni riservate da accessi non autorizzati.

11. Trattamenti e servizi in outsourcing o in contitolarietà

Adempimenti dei Delegati che si avvalgono di soggetti esterni

I Delegati che affidano trattamenti a soggetti esterni (ad esempio con appalto) o che svolgono trattamenti in contitolarietà con soggetti esterni (ad esempio convenzioni con altri enti pubblici), assicurano:

1. L'acquisizione e conservazione delle seguenti attestazioni:
   a) Sottoscrizione impegno di riservatezza, quando vengono affidate attività che si svolgono nei locali di ARPAT, ove il personale della ditta potrebbe venire a conoscenza di dati riservati o conversazioni riservate (ad esempio per servizi di pulizia, idraulica, elettricista, ecc.).
   b) Sottoscrizione misure di sicurezza e impegno di riservatezza, quando vengono affidate operazioni di maggiore criticità, senza gestione di dati personali, quali ad esempio:
      - accesso alla rete dati di ARPAT;
      - supporto su tecnologie altamente specialistiche, nelle quali il soggetto esterno potrebbe avere accesso a dati personali, senza entrare nel merito del significato dei dati.
   c) Nomina a Responsabile esterno, sottoscrizione misure di sicurezza e impegno di riservatezza, quando vengono affidate attività di trattamento ai sensi dell'art. 28 del GDPR.
   d) Sottoscrizione "accordo data protection" nei casi in cui il trattamento venga effettuato in concorso con un Titolare esterno, ai sensi dell'art. 26 del GDPR.
2. L'invio all'Ufficio DPO, per conservazione nel dossier data protection, della documentazione più rilevante ai fini della data protection, quale ad esempio quella relativa ai casi c, d di cui al precedente punto:

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

- 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).

3. L'attuazione delle misure necessarie a consentire la migrazione ad altro fornitore qualora l'oggetto del trattamento riguardi dati e informazioni strategiche per il funzionamento di ARPAT.
4. La verifica dell'operato del soggetto esterno.

Le modalità relative alla sottoscrizione di impegno di riservatezza, misure di sicurezza, alla nomina di Responsabile esterno e alla stipula dell'accordo di data protection, sono definite nei paragrafi successivi. Questi adempimenti non sono necessari se il soggetto esterno:

- non effettua alcun trattamento dati per ARPAT o in contitolarietà con ARPAT;
- non svolge alcuna attività nei locali di ARPAT;
- non accede alla rete dati di ARPAT.

Sottoscrizione impegno di riservatezza

Il soggetto esterno si impegna ad assicurare la riservatezza professionale propria e di tutto il personale eventualmente designato alla esecuzione del contratto (non rivelare informazioni o dati venuti a conoscenza nel corso dell'esecuzione del contratto mantenendole segrete).

Sottoscrizione misure di sicurezza

Le misure di sicurezza sono definite d'intesa con il Responsabile ICT.

Il soggetto esterno:

a) comunica gli estremi identificativi delle persone fisiche che svolgono le funzioni di supporto applicativo o amministratore di sistema nell'ambito del contratto in oggetto, con la descrizione delle funzioni ad esse attribuite e si impegna a comunicare tempestivamente ogni eventuale variazione;

b) si impegna ad assicurare il rispetto di misure di sicurezza adeguate alla tipologia di servizio fornito e alla tipologia di dati trattati, quali ad esempio:

   - protezione dei dati trattati mediante misure tecniche e organizzative tali da evitarne trattamenti non autorizzati, illeciti, perdita o distruzione;
   - rispetto delle basilari misure di sicurezza informatica da parte di tutto il personale del soggetto esterno designato allo svolgimento del servizio, quali ad esempio: non condividere le credenziali assegnate con altri utenti (qualora ciò accada, anche per

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

motivi fortuiti, cambiare password); utilizzare password sufficientemente robuste (8 caratteri contenenti anche numeri o caratteri speciali, 14 caratteri per amministratori) custodire diligentemente le credenziali; non lasciare incustodito e accessibile il dispositivo elettronico durante una sessione di collegamento alla rete di Arpat, bensì bloccare il computer; non divulgare, comunicare, cedere a terzi informazioni relative all'infrastruttura di Arpat; non svolgere attività che possano facilitare l'accesso ad essa da parte di personale non autorizzato, non manomettere la configurazione dei sistemi; attenersi alle istruzioni ricevute per l'accesso ai servizi; non tentare di accedere a servizi non consentiti, non tentare di acquisire privilegi di superuser o administrator; comunicare tempestivamente eventuali incidenti informatici e violazioni di dati.

Nomina a Responsabile esterno

I Delegati che si avvalgono di soggetti esterni all'Agenzia assicurano:

1. che il trattamento sia autorizzato preventivamente in forma scritta dal Titolare con nomina del Responsabile esterno (come da art. 28 comma 2 del GDPR);
2. che il trattamento sia conforme alle disposizioni contenute nel GDPR e D.Lgs. 196/2003, mediante adozione di misure di sicurezza adeguate alla tipologia e riservatezza dei dati trattati quali, ad esempio, clausole contrattuali che prevedano:
   a) sottoscrizione impegno di riservatezza e misure di sicurezza;
   b) obblighi di comunicazione, da parte del soggetto esterno, degli estremi identificativi del Responsabile del trattamento da questi effettuato;
   c) l'attestazione di conformità del trattamento alle disposizioni contenute nel GDPR e alle disposizioni di legge relative alla sicurezza dei sistemi informativi delle pubbliche amministrazioni (esempio misure minime di sicurezza) da parte del soggetto esterno;
   d) l'accettazione, da parte del soggetto esterno, delle regole stabilite nel presente Disciplinare, qualora il trattamento sia effettuato con strumenti ICT di ARPAT;
   e) la consegna, con periodicità adeguata alla tipologia di servizio fornito, dei dati significativi di backup da parte del soggetto esterno, ovvero dei dati necessari a poter migrare in autonomia ad altro fornitore;
   f) poteri di verifica, da parte di ARPAT, in merito alle modalità operative adottate per il trattamento da parte del soggetto esterno;
   g) applicazione di penali proporzionate alla gravità della mancanza qualora il trattamento effettuato non risulti conforme alle disposizioni impartite.

Accordo data protection di contitolarietà

Per i trattamenti effettuati in concorso con Titolari esterni (ad esempio a seguito di convenzione con altri enti pubblici) si stipula un "accordo data protection", ai sensi dell'art. 26 del GDPR.

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

L’accordo determina, in modo trasparente, le responsabilità dei contitolari in merito all’osservanza degli obblighi derivanti dal GDPR, con particolare riguardo alla definizione dei ruoli, compiti e responsabilità per garantire i diritti delle persone interessate.

Per la sua predisposizione si utilizza, come riferimento, la “Data protection policy - Linee guida per l’attuazione dei processi GDPR” di ARPAT.

Il contenuto essenziale dell’accordo è messo a disposizione degli interessati.

12. Accessibilità ai diversamente abili

I documenti che si creano nelle normali attività lavorative rispettano i requisiti di "accessibilità", ovvero sono fruibili indipendentemente dalla condizione di disabilità personale, applicando i criteri di accessibilità definiti dai requisiti tecnici di cui all’articolo 11 della legge 9 gennaio 2004, n. 4.

13. Formazione degli autorizzati

La formazione di base è assicurata mediante:

- comunicazione metodica ai nuovi assunti delle istruzioni relative all'utilizzo dei sistemi ICT, alle modalità per i trattamenti dati e diffusione di queste istruzioni sulla intranet;
- capillare diffusione del presente Disciplinare e della normativa interna su ICT e trattamenti dati;
- pubblicazione, sulla intranet, delle schede sistema descrittive dei singoli sistemi ICT in uso in Agenzia, che costituiscono la guida di riferimento per gli utenti;
- rilevazione dei bisogni formativi mediante periodici sondaggi;
- pubblicazione, sulla intranet, di corsi in materia di sicurezza informatica e privacy.

La formazione è effettuata al momento dell’ingresso del personale presso la struttura, nonché in occasione dei cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti rilevanti rispetto al trattamento dei dati.

Inoltre, sono programmati specifici interventi formativi con obbligo di partecipazione da parte del personale designato.

Articolo 11
Utilizzo della Posta elettronica

Il servizio di posta elettronica erogato dai sistemi di ARPAT è ad uso esclusivo di ARPAT.

Ogni comunicazione via posta elettronica con soggetti esterni o interni all'amministrazione deve avvenire esclusivamente mediante l’utilizzo del sistema di posta elettronica di ARPAT, per garantire i necessari livelli di sicurezza e riservatezza.

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

A tal fine ARPAT assegna una casella di posta personale a tutto il personale che ha un rapporto di lavoro con l'Agenzia e che risulti abile all'utilizzo del servizio. Gli assegnatari delle caselle di posta sono tenuti a consultarle, a gestirle e a ripulirle periodicamente dallo spam.

I messaggi trasmessi si intendono inviati e pervenuti ai destinatari se trasmessi agli indirizzi di posta loro assegnati (nel caso si tratti di personale interno e quindi di caselle del dominio ARPAT) o dichiarati (nel caso si tratti di soggetti esterni). Quanto alla certezza della ricezione del messaggio da parte del destinatario, il mittente, ove ritenuto necessario, può richiedere al destinatario stesso un messaggio di risposta che confermi l'avvenuta ricezione.

L’assegnazione delle caselle di posta elettronica ai dipendenti è finalizzata all’utilizzo di tale mezzo di comunicazione per lo svolgimento dell’attività lavorativa. Ad esempio non è consentito utilizzare l'indirizzo di posta elettronica aziendale per:

- motivi non attinenti allo svolgimento delle mansioni assegnate;
- la partecipazione a dibattiti, forum o mailing list su Internet per motivi non professionali;
- aderire o rispondere a messaggi che invitano a perpetuare verso ulteriori indirizzi di posta elettronica contenuti o documenti oggetto delle cosiddette “catene di S. Antonio”;
- effettuare ogni genere di comunicazione finanziaria ivi comprese le operazioni “remote banking”, acquisti on-line e simili, salvo diversa ed esplicita autorizzazione aziendale.

Inoltre, non è consentito:

- simulare l'identità di un altro utente, ovvero utilizzare credenziali di posta non proprie per l'invio di messaggi;
- prendere visione della posta altrui;
- aprire messaggi di posta ambigui e di incerta provenienza (gli allegati possono infatti contenere virus o codici nascosti di natura dolosa che possono comportare la divulgazione di password o il danneggiamento di dati);
- l'invio a mezzo posta elettronica di dati particolari, personali e/o commerciali di alcun genere se non nel rispetto delle norme sulla disciplina del trattamento e della protezione dei dati personali;
- divulgare contenuti illeciti o altrimenti inaccettabili, oppure finalizzati a violare i diritti legali altrui.

Articolo 12
Utilizzo di Internet

Il collegamento a Internet, reso disponibile sulle postazioni di lavoro, è finalizzato all’utilizzo di tale mezzo di comunicazione per lo svolgimento dell’attività lavorativa. Ad esempio non è consentito:

- navigare in siti Internet non attinenti allo svolgimento delle mansioni assegnate;

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

- effettuare ogni genere di transazione finanziaria ivi comprese le operazioni “remote banking”, acquisti on-line e simili, salvo diversa ed esplicita autorizzazione aziendale;
- lo scarico di software prelevati dai siti Internet, salvo diversa ed esplicita autorizzazione aziendale;
- ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
- la partecipazione, per motivi non professionali, a forum, chat line, bacheche elettroniche, registrazioni in guest book, anche utilizzando pseudonimi (nickname);
- scaricare materiale di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, condizioni di salute, opinione e appartenenza sindacale e/o politica.

Articolo 13
Utilizzo della intranet e del sito web

La intranet e il sito web sono i principali strumenti utilizzati per pubblicare o condividere in sicurezza contenuti in rete (quali informazioni, notizie, documenti, comunicazioni, decreti, procedure, manuali, ecc.) che riguardano i trattamenti dati effettuati da ARPAT.

Si utilizza la intranet per la pubblicazione o condivisione di contenuti che interessano tutto il personale dell'Agenzia o specifiche categorie di utenti interni.

Si utilizza il sito web per la pubblicazione di contenuti che interessano i cittadini o specifiche categorie di soggetti esterni all'Agenzia.

Tramite la intranet e il sito web è inoltre possibile accedere ai principali applicativi e servizi di rete basati su tecnologia web.

I file che vengono inseriti nella intranet e nel sito web devono essere prodotti preferibilmente con strumenti open source.

Articolo 14
Tipologia delle informazioni memorizzate relative all'utilizzo delle risorse ICT, finalità e modalità di gestione

1. Informazioni memorizzate relative a telefonia di rete fissa, telefonia mobile, telefonia via Internet, posta elettronica, accesso a Internet

Sono memorizzate da parte di ARPAT le seguenti informazioni ove ciò sia possibile:

1. i dati necessari per rintracciare e identificare la fonte di una comunicazione;
2. i dati necessari per rintracciare e identificare la destinazione di una comunicazione;
3. i dati necessari per determinare la data, l'ora e la durata di una comunicazione;

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

4. i dati necessari per determinare il tipo di comunicazione;
5. i dati necessari per determinare le attrezzature di comunicazione degli utenti o quello che si presume essere le loro attrezzature.

2. Informazioni memorizzate relative ad altri servizi ICT

Sono memorizzate da parte di ARPAT le seguenti informazioni ove ciò sia possibile:

1. i dati necessari per determinare la data, l'ora e la durata di accesso al servizio;
2. i dati necessari per determinare il tipo di servizio utilizzato;
3. i dati necessari per identificare il tipo di operazioni effettuate;
4. i dati necessari per determinare le attrezzature utilizzate per accedere al servizio;
5. ulteriori dati qualora siano previsti da specifiche leggi, norme o regolamenti di settore.

3. Finalità delle informazioni salvate e durata della conservazione

Le informazioni di cui ai precedenti paragrafi a) e b) sono tracciate e conservate per finalità organizzative di sicurezza e di controllo da parte dell'Agenzia per i periodi minimi e massimi stabiliti dalle norme vigenti.

Articolo 15
Controlli e sanzioni

A garanzia della sicurezza dei sistemi informativi e dei servizi di rete, è nella facoltà di ARPAT effettuare controlli preliminari su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree, nonché predisporre controlli a campione, in forma anonima, sull'utilizzo delle risorse ICT per le quali è riconosciuto il diritto del lavoratore (e dei terzi) a una sfera di riservatezza anche nelle relazioni lavorative, come ad esempio nell'uso della posta elettronica, nell'accesso a Internet/intranet, nell'uso delle condivisioni personali e servizi ad essi assimilabili.

È sempre fatta salva l'ipotesi dell'attivazione di controlli, anche individualizzati, che trovino giustificazione nelle seguenti necessità:

- corrispondere a eventuali richieste di organi di polizia su segnalazione dell'autorità giudiziaria;
- nel verificarsi di un evento dannoso o una situazione di pericolo che richieda un immediato intervento;
- nella presenza di sospetti relativamente all'esistenza di condotte improprie nell'uso delle apparecchiature;
- specifiche richieste dell'interessato relative a dati che lo riguardano.

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

A garanzia della sicurezza dei sistemi informativi, dei servizi di rete e dei dati aziendali è, tuttavia, nella facoltà di ARPAT effettuare controlli puntuali sulla applicazione delle norme contenute nel presente Disciplinare che non riguardano la sfera di riservatezza riconosciuta al lavoratore (quali ad esempio il rispetto delle norme generali di comportamento, la verifica dell'operato degli amministratori di sistema, ecc.) da parte dei Delegati.

ARPAT non effettuerà trattamenti di dati personali mediante sistemi hardware e/o software che mirino al controllo a distanza dei lavoratori quali:

- lettura e/o registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
- riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore.

Nei casi di accertata violazione dei principi fissati nel presente Disciplinare, è demandata ai singoli dirigenti preposti l’applicazione dei provvedimenti disciplinari individuati nel CCNL con le modalità ivi previste per il personale dipendente o equiparato, l’applicazione delle sanzioni previste nelle clausole contrattuali per i soggetti non dipendenti.

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

Allegato 1
Compiti aggiuntivi dei Delegati

(ai sensi dell'art. 29 del Decreto legislativo 30 giugno 2003, N. 196 e dell'art. 9 del Disciplinare ICT e trattamenti dati Rev. 01)

Ai Delegati individuati nel presente Allegato:

- Direttore amministrativo
- Direttore tecnico
- Coordinatori di Area Vasta
- Responsabili dei dipartimenti che non sono sede di Area Vasta
- Responsabile Settore SIRA
- Responsabile Settore Affari generali
- Responsabile Settore Gestione delle risorse umane
- Responsabile Settore Patrimonio immobiliare impianti e reti
- Responsabili dei Settori Attività amministrative e Provveditorato

sono assegnati specifici compiti aggiuntivi, necessari ad assicurare adeguato livello di tutela dei dati e delle informazioni trattate, che si aggiungono a quelli già definiti all'art. 9 del Disciplinare.

1. Direttore amministrativo

Assicura che l’accesso in Agenzia presso la Direzione avvenga in modo controllato.

2. Direttore tecnico

Cura il coordinamento della predisposizione delle proposte di investimento relative alla dotazione tecnologica dell’Agenzia in coerenza con:

- Politica per l'ICT e i trattamenti dati;
- contenuti della Relazione sull'ICT.

3. Coordinatori di Area Vasta

Assicurano d'intesa con il Settore SIRA, presso la sede dell'Area vasta di competenza, il rispetto delle politiche di sicurezza relative alla gestione delle infrastrutture di supporto e alla protezione delle aree e dei locali, con particolare riferimento a quanto segue:

- controllo degli accessi ai locali della sede;

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

- gestione operativa dei servizi di supporto necessari al corretto funzionamento dei sistemi informatici (rete dati, energia elettrica, condizionamento, sistemi antincendio, servizi di videosorveglianza);
- gestione operativa, in collaborazione con il Settore SIRA, dei beni ICT dislocati presso la sede;
- protezione degli apparati critici (quali ad esempio i server e altri apparati critici dislocati presso la sede);
- protezione dei cablaggi critici come le dorsali della rete dati e i cavi di alimentazione degli apparati critici (server e impianti ausiliari).

Assicurano, presso la Area vasta di competenza, il controllo sulla attuazione del Disciplinare ICT e trattamenti dati.

4. Responsabili dei dipartimenti che non sono sede di Area Vasta

Assicurano d'intesa con il Settore SIRA, presso la sede di competenza, il rispetto delle politiche di sicurezza relative alla gestione delle infrastrutture di supporto e alla protezione delle aree e dei locali, con particolare riferimento a quanto segue:

- controllo degli accessi ai locali della sede;
- gestione operativa dei servizi di supporto necessari al corretto funzionamento dei sistemi informatici (rete dati, energia elettrica, condizionamento, sistemi antincendio, servizi di videosorveglianza);
- gestione operativa, in collaborazione con il Settore SIRA, dei beni ICT dislocati presso la sede;
- protezione degli apparati critici (quali ad esempio i server e altri apparati critici dislocati presso la sede);
- protezione dei cablaggi critici come le dorsali della rete dati e i cavi di alimentazione degli apparati critici (server e impianti ausiliari).

5. Responsabile Settore SIRA

È il Responsabile ICT e il Responsabile dell'Ufficio DPO.

Assicura il rispetto delle politiche di sicurezza relative alla gestione operativa dei beni ICT dislocati presso la Direzione.

Tali compiti sono svolti avvalendosi del Responsabile per la transizione al digitale (RTD).

6. Responsabile Settore Affari generali

Verifica la conformità dal punto di vista formale dei decreti alla normativa in materia di data protection, in particolare verifica se l'atto contiene le seguenti obbligatorie indicazioni:

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

a) l'indicazione del trattamento dati cui è riconducibile l'atto con riferimento al Registro Trattamenti;

b) l'indicazione se l'atto è rilevante o meno ai fini della data protection;

c) qualora sia affermata la rilevanza ai fini della data protection, l'indicazione dei seguenti ulteriori obbligatori elementi:

c.1) la categoria di data protection alla quale l'atto è riconducibile tra quelle indicate all'art. 10.2 e) del presente Disciplinare, ovvero:

i. attivazione di trattamenti con nuovi sistemi informatici e/o tecnologie;

ii. affidamento di trattamenti dati a soggetti esterni con nomina Responsabile;

iii. svolgimento di attività insieme a soggetti esterni, con accordo di contitolarietà;

iv. normativa ICT e trattamenti dati, misure di sicurezza;

v. Registro trattamenti;

vi. DPIA;

b,2) l'impegno del proponente o del RUP, se diverso dal proponente, a notificare l'atto dopo l'approvazione all'Ufficio DPO per conservazione nel dossier data protection;

b.3) qualora l'atto appartenga alla categoria data protection "attivazione di trattamenti con nuovi sistemi informatici e/o tecnologie", il parere del Responsabile ICT / Ufficio DPO che attesta la conformità alla normativa su data protection e ICT.

7. Responsabile Settore Gestione delle risorse umane

Cura le seguenti attività:

1. comunicazione ai nuovi assunti di una nota informativa, predisposta dal Settore SIRA, in materia di utilizzo dei sistemi informatici, telefonia e tutela della privacy;
2. comunicazione delle assunzioni, cessazioni, trasferimenti, nomine dei Responsabili al Settore SIRA, al Settore Provveditorato, ai Settori Amministrativi;
3. organizzazione e programmazione dei corsi in materia di sicurezza informatica e privacy previsti nel piano di formazione;
4. rendicontazione dei corsi effettuati in materia di sicurezza informatica e privacy.

8. Responsabile Settore Patrimonio immobiliare impianti e reti

Assicura, d'intesa con il Responsabile Settore SIRA, il rispetto delle politiche per la gestione delle infrastrutture di supporto e la protezione delle aree e dei locali relativamente a quanto segue:

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

1. servizi di supporto al funzionamento dei sistemi informatici (rete dati, energia elettrica, condizionamento, sistemi antincendio, servizi di videosorveglianza);
2. protezione degli apparati critici (server, apparati di rete, ecc. in locali climatizzati, protetti da accessi non autorizzati, dotati di sistemi antincendio).
3. protezione dei cablaggi critici come le dorsali della rete dati e i cavi di alimentazione degli apparati critici (server e impianti ausiliari).

Cura la gestione operativa delle attività che riguardano le infrastrutture di supporto e la protezione delle aree e dei locali presso la sede della Direzione, relativamente agli aspetti sopra indicati.

9. Responsabili dei Settori Attività amministrative e Provveditorato

Assicurano, in qualità di consegnatari:

1. la tenuta di un inventario aggiornato dei beni ICT di competenza, in stretto raccordo con il Settore SIRA, nonchè con gli utilizzatori dei beni informatici, che a tale proposito sono tenuti a fornire tempestivamente ogni utile informazione relativa alla gestione inventariale di tali beni;
2. che i beni ICT di competenza siano restituiti ad ARPAT alla cessazione dell'esigenza per la quale erano stati previsti (ad esempio alla cessazione dell'incarico, del rapporto di lavoro, del rapporto di collaborazione, del rapporto contrattuale con ARPAT o a seguito di trasferimento presso altra struttura di ARPAT).

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

Allegato 2
Norme generali di comportamento prescritte agli autorizzati

(ai sensi dell'art. 10 del presente Disciplinare ICT)

1. Disposizioni generali sull'utilizzo dei sistemi ICT e sui trattamenti dati

Ciascun autorizzato effettua i trattamenti dati relativi alle funzioni cui è assegnato attenendosi a quanto segue.

1. Principi generali e norme di comportamento

a) norme contenute nel presente Disciplinare;

b) norme di comportamento contenute nel presente allegato;

c) principi generali e finalità su cui si basa l'utilizzo delle risorse ICT e il trattamento dei dati aziendali (definiti nell'art. 4 del Disciplinare ed esplicitati nella Politica per l'ICT e i trattamenti dati di ARPAT) di seguito richiamati:

   i. diligenza e correttezza nell'uso degli strumenti ICT;

   ii. utilizzare le risorse ICT dell'Agenzia unicamente per perseguire gli scopi lavorativi;

   iii. adeguata protezione dei dati e delle informazioni, in maniera da evitare trattamenti non autorizzati, illeciti, perdita o distruzione;

   iv. il rispetto delle regole è necessario per assicurare il corretto funzionamento degli strumenti informatici e consentire ad ARPAT di conseguire gli obiettivi di efficienza, efficacia ed economicità;

   v. favorire la trasparenza, l'accountability, la partecipazione, l'efficacia dell'azione amministrativa;

   vi. assicurare la riservatezza professionale nelle istruttorie riservate (ad esempio quelle relative alle attività amministrativa e sanzionatoria);

   vii. favorire la diffusione delle informazioni di interesse pubblico attraverso i canali previsti;

   viii. rispettare i principi della normativa sulla protezione dei dati personali, stabiliti per i trattamenti dati: liceità, correttezza, trasparenza, limitazione delle finalità in base alle quali si raccolgono i dati (determinate, esplicite e legittime), minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza;

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

2. Disposizioni sulla data protection

Registro Trattamenti

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. Eventuali deroghe richiedono autorizzazione scritta del Titolare e contestuale aggiornamento del Registro;

Diritti degli interessati (da art. 12 a art. 23 del GDPR)

Tutto il personale organizza le attività assegnate in modo da consentire e semplificare il rispetto dei diritti degli interessati e attuare, ciascuno nell'ambito delle proprie competenze, misure per:

a) minimizzare i dati trattati;

b) proteggerli da accessi non consentiti;

c) consentire e semplificare l'individuazione dei dati che afferiscono ai singoli interessati;

d) soddisfare le richieste degli interessati relative all'accesso ai loro dati;

e) rispettare i termini ultimi di cancellazione previsti dal Manuale di gestione del protocollo informatico, dei documenti e dell'archivio di ARPAT;

f) informare gli interessati sulle modalità di trattamento (fare riferimento alla specifica informativa applicabile, come indicato nel seguito);

Informativa privacy

Tutto il personale è tenuto a:

a) conoscerla (consultare http://www.arpat.toscana.it/utilita/privacy);

b) farvi riferimento in ogni forma di comunicazione con l'esterno e con l'interno per far sapere agli interlocutori come vengono trattati i loro dati (seguire le istruzioni indicate in apposita Circolare del Direttore generale);

c) fornire agli interlocutori informative più specifiche nei casi in cui si attivino raccolte sistematiche di dati personali tematici non indicati in essa.

Furti, perdita o distruzione di dispositivi contenenti dati

Occorre che il lavoratore, dopo aver provveduto alle denunce e segnalazioni d'obbligo, rilasci una dichiarazione al proprio dirigente o direttamente all'Ufficio DPO come da para 3.8.3 della Procedura ICT.

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

5. Disposizioni sull’accessibilità ai diversamente abili

I documenti che si creano nelle normali attività lavorative rispettano i requisiti di "accessibilità", ovvero sono fruibili indipendentemente dalla condizione di disabilità personale, applicando i criteri di accessibilità definiti dai requisiti tecnici di cui all’articolo 11 della legge 9 gennaio 2004, n. 4.

A tal fine utilizzare i modelli di carta intestata e documento/relazione presenti nella intranet, seguendo le istruzioni in essi contenute.

6. Disposizioni sui sistemi ICT e disposizioni del preposto Responsabile

Ciascun autorizzato è personalmente responsabile del corretto utilizzo dei sistemi ICT che gli sono stati affidati e dei dati che inserisce o modifica negli applicativi.

Inoltre è tenuto a:

a) acquisire le nozioni di base sulla sicurezza informatica e la protezione dei dati consultando le informazioni iniziali per i nuovi assunti sull'utilizzo dei sistemi informatici, telefonia e tutela della privacy e frequentando i corsi cui è invitato a partecipare;

b) comunicare tempestivamente a tic@arpat.toscana.it , eventualmente tramite il Responsabile della struttura cui è assegnato, ogni evento rilevante ai fini della protezione dei dati e della sicurezza ICT;

c) attenersi alle regole di utilizzo dei singoli sistemi ICT impiegati per l'espletamento delle proprie attività lavorative, contenute nelle “Schede sistema” dei sistemi utilizzati (ad esempio: posta elettronica, protocollo informatico, sito web istituzionale, intranet, ecc.);

d) attenersi alle eventuali ulteriori istruzioni del preposto Responsabile.

2. Misure di sicurezza nei trattamenti dati con l'ausilio di strumenti elettronici

Ogni autorizzato che tratta dati con gli strumenti elettronici è vincolato alle seguenti norme generali di comportamento:

1. non condividere il proprio account con altri utenti (a meno che non sia espressamente previsto);
2. non cedere a terzi la propria password, a meno che ciò non sia espressamente previsto; qualora ciò accada, anche per motivi fortuiti, richiedere il reset della password al referente dell’applicativo;
3. utilizzare password di almeno 8 caratteri non facilmente riconducibili all’autorizzato, contenenti anche numeri o caratteri speciali; nel caso in cui lo strumento elettronico non lo consenta, la password dovrà essere composta dal numero di caratteri pari al massimo consentito; per le utenze amministrative è richiesta maggiore robustezza (almeno 14 caratteri contenenti anche numeri e caratteri speciali);

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

4. cambiare la password al primo utilizzo e successivamente almeno ogni 3 mesi;
5. non lasciare incustodito e accessibile lo strumento elettronico durante una sessione del trattamento, bensì bloccare il computer e, inoltre, configurare il salvaschermo nella modalità di attivazione automatica;
6. non lasciare incustoditi e accessibili i dispositivi portatili;
7. salvare i dati e i documenti sui server;

   Note:

   a) per il salvataggio utilizzare gli appositi servizi di rete cui si è abilitati, quali ad esempio:

      - condivisioni di rete;
      - intranet;
      - sito web;
      - sistema di protocollo informatico e gestione documentale;
      - altri applicativi di rete.

   b) è altresì possibile salvare copie di lavoro dei dati e dei documenti non riservati sulle postazioni di lavoro e sui dispositivi mobili aziendali (notebook, smartphone, tablet, ecc.);

   c) è altresì possibile salvare copie di lavoro dei dati e dei documenti riservati su supporti removibili aziendali a condizione di rispettare le misure previste per i trattamenti dei dati particolari giudiziari o comunque riservati (vedi successivo paragrafo 4);

8. navigazione Internet: non visitare / scaricare / eseguire file da siti poco sicuri;
9. posta elettronica: non aprire alcun allegato sospetto né seguire collegamenti sospetti, dove per sospetto si intende non atteso e/o proveniente da mittenti sconosciuti;
10. conoscere le caratteristiche dei sistemi e servizi informatici utilizzati e attenersi alle norme di utilizzo se presenti (le quali sono contenute nelle schede sistema, pubblicate sulla intranet);
11. non eseguire o installare software senza autorizzazione da parte della struttura responsabile dell'ICT e senza verifica che tale software sia libero da virus;
12. non tentare di accedere a servizi loro non consentiti;
13. non tentare di acquisire privilegi di superuser o administrator;
14. non collegare modem o comunque dispositivi che consentano un accesso non controllato a Internet o ad apparati (router, sistemi di elaborazione, personal computer connessi in rete, ecc.) della rete privata di ARPAT;

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

15. spegnere i propri strumenti di lavoro al termine della giornata lavorativa a meno che non vi siano diverse motivate disposizioni contrarie;
16. non intercettare, alterare, impedire o interrompere comunicazioni di altri utilizzatori o servizi della Rete; non installare apparecchiature idonee a tale scopo, salvo che queste attività non siano atte a garantire le previste misure di sicurezza di ARPAT;
17. nei casi dubbi (su come comportarsi) chiedere chiarimenti e/o istruzioni eventualmente scritte al competente Responsabile.

3. Misure di sicurezza nei trattamenti dati senza l'ausilio di strumenti elettronici

1. Custodire e controllare, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti avuti in carico contenenti dati personali e altre tipologie di dati e assicurare che siano restituiti al termine delle operazioni affidate;
2. Assicurare che agli atti e documenti avuti in carico che contengano dati o informazioni riservate non accedano persone prive di autorizzazione;
3. Assicurare che:
    - l'accesso agli archivi contenenti dati o informazioni riservate sia controllato;
    - le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, siano identificate e registrate;
    - quando gli archivi non siano dotati di strumenti elettronici per il controllo degli accessi o di autorizzati della vigilanza, le persone che vi accedono siano preventivamente autorizzate.
4. nei casi dubbi (su come comportarsi) chiedere chiarimenti e/o istruzioni eventualmente scritte al competente Responsabile.

4. Misure di sicurezza nei trattamenti di dati riservati

I dati riservati includono i dati personali che nel GDPR sono definiti dati particolari e dati relativi a condanne penali e reati e qualunque altra tipologia di dato definito riservato dal competente Delegato o nella scheda descrittiva del sistema (scheda sistema).

I trattamenti di dati riservati richiedono esplicita autorizzazione scritta da parte del competente Responsabile che, nel caso di dati particolari e giudiziari, verifica che il trattamento si svolga nel rispetto del Decreto del Presidente della Giunta Regionale n. 18 del 18.5.2006 (Regolamento sul trattamento dei dati sensibili e giudiziari).

Per i trattamenti di dati riservati valgono le seguenti regole aggiuntive:

1. utilizzare sistemi applicativi abilitati al trattamento delle suddette tipologie di dati.

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

2. effettuare trattamenti con strumenti di Office Automation o altri strumenti di produttività personale esclusivamente se i dati risiedono:
    - in una apposita cartella ubicata su un server, ove possa accedere il solo personale abilitato secondo la procedura prevista dal servizio di condivisione delle risorse;
    - su supporti rimovibili aziendali criptati conservati e gestiti come indicato nel seguito;
3. custodire e conservare gli eventuali supporti rimovibili utilizzati per memorizzare i dati in armadi chiusi a chiave o secondo le eventuali disposizioni scritte impartite dal competente Responsabile;
4. svolgere le azioni necessarie ad assicurare che i supporti removibili non più utilizzati, che hanno contenuto dati riservati, siano distrutti o resi inutilizzabili, salvo seguire apposite disposizioni al riguardo, approvate dal Responsabile ICT;
5. nei casi dubbi (su come comportarsi) chiedere chiarimenti e/o istruzioni scritte al competente Responsabile.

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