

**ARPAT - DIREZIONE GENERALE**

*Via Ponte alle Mosse, 211 - 50144 - Firenze*

---

# **Informativa specifica relativa ai trattamenti effettuati mediante le piattaforme finalizzate a garantire la sicurezza informatica**

(ai sensi degli articoli 12, 13 e 14 del Regolamento (UE) 2016/679)

## Sommario

1. Scopo .....	3
2. Titolare e Responsabile della protezione dei dati personali .....	3
3. Finalità e base giuridica dei trattamenti .....	3
3.1 Finalità di Arpat (titolare) .....	3
3.2 Finalità dei fornitori (titolari autonomi) .....	4
4. Interessati, dati trattati, destinatari e trasferimenti dati .....	5
4.1 Categorie degli interessati .....	5
4.2 Categorie di dati personali trattati .....	5
4.3 Categorie di destinatari a cui i dati personali possono essere comunicati .....	6
4.4 Trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale	6
5. Modalità dei trattamenti dati .....	6
5.1 Generalità sui trattamenti e periodo di conservazione dei dati .....	6
5.2 Luogo dei trattamenti .....	7
5.3 Protezione dei dati .....	7
6. Diritti degli interessati .....	7
7. Diritto di reclamo .....	7

## 1. Scopo

La presente informativa descrive i trattamenti di dati personali effettuati tramite le piattaforme per garantire la postura di sicurezza informatica quali EMS (Endpoint Management System), NAC (Network Access Control), XDR (Extended Detection and Response), FortiAnalyzer e SIEM (Security Information and Event Management) utilizzate da ARPAT per garantire la sicurezza dei sistemi informativi, della rete e dei dispositivi dell'Agenzia.

Le piattaforme sono fornite da soggetti terzi: Fortinet (EMS, NAC e FortiAnalyzer) e Trend Micro (XDR e SIEM).

E' resa ai sensi degli articoli 12, 13 e 14 del Regolamento (UE) 2016/679 (noto come GDPR).

## 2. Titolare e Responsabile della protezione dei dati personali

Rimangono validi i riferimenti indicati nell'informativa generale.

Poiché le piattaforme EMS, NAC, XDR, FortiAnalyzer e SIEM sono fornite da soggetti terzi che trattano dati personali sui propri sistemi e infrastrutture, si precisa che:

- ARPAT rimane titolare del trattamento dei dati personali trattati nell'ambito delle proprie finalità connesse alla sicurezza informatica;
- Fortinet Inc. (EMS, NAC, FortiAnalyzer) e Trend Micro (XDR e SIEM) operano come titolari autonomi per i trattamenti effettuati sui propri servizi cloud e infrastrutture per finalità proprie, in particolare per telemetria, diagnostica, miglioramento dei servizi e gestione delle minacce su scala globale.

## 3. Finalità e base giuridica dei trattamenti

### 3.1 Finalità di Arpat (titolare)

- a) garantire la sicurezza dei sistemi informativi e della rete per aumentare la resilienza de sistemi;
- b) monitorare l'integrità dei dispositivi e verificarne la conformità alle policy interne;

- c) prevenire incidenti informatici, intrusioni e attività anomale;
- d) rispondere a minacce, vulnerabilità o compromissioni;
- e) garantire la continuità operativa e l'integrità dei sistemi informativi dell'Agenzia.

### 3.2 Finalità dei fornitori (titolari autonomi)

Fortinet e Trend trattano dati anche per le seguenti finalità tecniche:

- a) funzionamento del servizio e telemetria;
- b) analisi delle minacce su scala globale;
- c) miglioramento degli algoritmi di rilevamento;
- d) monitoraggio delle prestazioni del sistema.

La base giuridica dei trattamenti è costituita da:

- art. 6, par. 1, lett. e) del Regolamento (UE) 2016/679 – trattamento necessario per l'esecuzione dei compiti istituzionali di ARPAT;
- le misure tecniche e organizzative previste dagli artt. 32–34 del Regolamento (UE) 2016/679.

Tali compiti sono disciplinati e specificati, in particolare, dalla normativa in materia di digitalizzazione, sicurezza ICT e cybersicurezza, nonché dalle disposizioni organizzative interne dell'Agenzia, quali:

- il Codice dell'Amministrazione Digitale (D.lgs. 82/2005);
- la Direttiva (UE) 2022/2555 (NIS2) e il D.lgs. 4 settembre 2024, n. 138;
- la Legge 28 giugno 2024, n. 90;
- il Piano Triennale per l'informatica nella Pubblica Amministrazione;
- le Linee guida adottate da AgID;
- le disposizioni interne che regolano l'organizzazione e la sicurezza dei sistemi informativi dell'Agenzia;
- le determinazioni e le linee guida adottate dall'Agenzia per la Cybersicurezza Nazionale (ACN), in attuazione del D.lgs. 4 settembre 2024, n. 138 e della Legge 28 giugno 2024, n. 90.

Per i trattamenti effettuati dai fornitori in qualità di titolari autonomi, le basi giuridiche sono individuate nelle rispettive informative privacy.

## **4. Interessati, dati trattati, destinatari e trasferimenti dati**

### **4.1 Categorie degli interessati**

Sono interessati dai trattamenti:

- a) personale di ARPAT (dipendenti, collaboratori, consulenti);
- b) personale di enti o imprese che accedono alla rete o ai sistemi ARPAT tramite account autorizzati;
- c) utenti connessi alla rete istituzionale, anche tramite VPN o accessi temporanei.

### **4.2 Categorie di dati personali trattati**

In funzione delle tecnologie utilizzate, possono essere trattati:

- credenziali digitali e identificativi dell'account (username, ID account);
- log di autenticazione e autorizzazione;
- indirizzi IP, MAC address, hostname, tipologia e stato dei dispositivi;
- dati relativi alla postura di sicurezza dei dispositivi (patch, antivirus, configurazioni);
- indicatori di compromissione e telemetrie di sicurezza;
- eventi di rete, log di accesso ai sistemi, rilevazioni di minacce;
- dati di navigazione di rete;
- dati necessari all'analisi degli incidenti di sicurezza.

Non vengono trattati dati personali particolari, salvo eventuale trattamento indiretto e occasionale derivante dalla gestione di incidenti di sicurezza o log applicativi, comunque gestiti nel rispetto delle norme sulla protezione dei dati.

### **4.3 Categorie di destinatari a cui i dati personali possono essere comunicati**

I dati possono essere comunicati a:

- soggetti interni autorizzati al trattamento (personale ICT autorizzato e preposto alla gestione della sicurezza informatica);
- fornitori esterni che erogano servizi di manutenzione, assistenza o monitoraggio delle piattaforme, nominati Responsabili del trattamento ai sensi dell'art. 28 GDPR;
- autorità pubbliche competenti, ivi incluse le autorità in materia di cybersicurezza, protezione dei dati personali e polizia giudiziaria, nei soli casi previsti dalla legge.

### **4.4 Trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale**

I trattamenti sono effettuati principalmente all'interno dello Spazio Economico Europeo. Eventuali trasferimenti verso paesi terzi da parte dei fornitori sono realizzati nel rispetto degli artt. 44–49 del GDPR.

## **5. Modalità dei trattamenti dati**

### **5.1 Generalità sui trattamenti e periodo di conservazione dei dati**

I dati sono trattati mediante strumenti informatici, algoritmi di sicurezza e infrastrutture specializzate. I sistemi possono effettuare analisi comportamentali, rilevamento automatico delle minacce e correlazione degli eventi.

In particolare, le principali attività comprendono:

- raccolta e analisi di log e telemetrie;
- correlazione degli eventi di sicurezza e individuazione di anomalie;
- applicazione di policy di accesso e sicurezza della rete;
- blocco di dispositivi o attività potenzialmente dannose;
- gestione della risposta agli incidenti.

ARPAT conserva i dati per il tempo strettamente necessario al conseguimento delle finalità di sicurezza, e comunque:

- i log sono conservati secondo i tempi previsti dalle policy ICT;
- i dati relativi a incidenti di sicurezza sono conservati fino alla conclusione delle verifiche e per il tempo necessario a documentarne la gestione.

I fornitori conservano i dati per i periodi indicati nelle loro privacy policy e nei contratti.

## 5.2 Luogo dei trattamenti

I trattamenti sono effettuati presso le sedi ARPAT e nei data center autorizzati indicati nella documentazione dei sistemi ICT.

## 5.3 Protezione dei dati

Sono adottate misure tecniche e organizzative idonee a prevenire accessi non autorizzati, perdita dei dati, diffusione o trattamenti non consentiti.

## 6. Diritti degli interessati

Restano validi i diritti indicati nell'informativa generale (accesso, rettifica, cancellazione, limitazione, opposizione), esercitabili tramite il Responsabile della protezione dei dati.

L'esercizio dei diritti potrà essere valutato caso per caso, tenendo conto delle esigenze di sicurezza dei sistemi informativi e della protezione dell'infrastruttura ICT.

Per i trattamenti effettuati da Fortinet e Trend in qualità di titolari autonomi, gli interessati possono consultare le rispettive informative e canali di contatto.

## 7. Diritto di reclamo

Resta valido quanto previsto nell'informativa generale con riferimento al Garante per la protezione dei dati personali.