Notifica di una violazione dei dati personali (*data breach*)

(art. 33 del Regolamento (UE) 2016/679 - art. 26 del D.Lgs 51/2018)

A) Dati del soggetto che effettua la notifica

Il sottoscritto Cognome: Pecis Nome: Ivano
E-mail: amministrazione@ip-privacy.it
nella sua qualità di
☐ rappresentante legale o ☒ delegato del rappresentante legale
Cognome: Petey Nome: Loredana

notifica la seguente violazione di dati personali e ☒ dichiara di aver preso visione dell'informativa sul trattamento dei dati personali e di essere consapevole che chiunque, in un procedimento dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi ne risponde ai sensi dell'art. 168 del Codice in materia di protezione dei dati personali (*Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante*) o dell'art. 44 del d.lgs. 51/2018 (*Falsità in atti e dichiarazioni al Garante*), salvo che il fatto non costituisca più grave reato. Il soggetto che effettua la notifica mediante la sottoscrizione e/o invio della stessa si assume la responsabilità della veridicità delle informazioni comunicate. La falsità nelle comunicazioni al Garante rappresenta un illecito penale ai sensi dell'art. 168 del d.lgs. 196/03 o ai sensi dell'art. 44 del d.lgs. 51/2018.

B) Tipo di notifica

Prima Notifica

- ☐ a) Completa
- ☒ b) Preliminare

La notifica viene effettuata

- ☒ ai sensi dell'art. 33 RGPD
- ☐ ai sensi dell'art. 26 d.lgs 51/2018

Notifica integrativa

- ☐ c) Integrativa

C) Titolare del trattamento

1. Il titolare del trattamento è:

☐ a)Censito nell'Indice nazionale dei domicili digitali delle imprese e dei professionisti
(INI-PEC www.inipec.gov.it - art. 6-bis Codice Amministrazione Digitale - D.Lgs n. 82/2005)

☒ b) Censito nell'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi -
(Tipologie Enti: Pubbliche Amministrazioni)
(IPA www.indicepa.gov.it - art. 6-ter Codice Amministrazione Digitale - D.Lgs n. 82/2005)

☐ c) Non censito in nessuno dei due precedenti indici

2. Dati del Titolare del trattamento:

Denominazione:	Comune di Aymavilles
Codice Fiscale/P.IVA:	00099010076
Stato:	Italia
Provincia:	Valle d'Aosta/Vallée d'Aoste
Comune:	Aymavilles
CAP:	11010
Indirizzo:	Chef Lieu N 1
Telefono:	0165922800
Email:	protocollo@pec.comune.aymavilles.ao.it
Pec:	protocollo@pec.comune.aymavilles.ao.it

D) Dati di contatto per informazioni relative alla violazione

1) Responsabile della protezione dei dati

☐ i cui dati di contatto sono stati già comunicati con la comunicazione prot. n

☒ i cui dati di contatto sono stati già comunicati al Garante, ma al momento non si dispone del numero di protocollo della relativa comunicazione:

Cognome:	Pecis
Nome:	Ivano
Email:	amministrazione@ip-privacy.it
Recapito telefonico per eventuali comunicazioni :	3792003377

2) Altro soggetto

Cognome:
Nome:
Email:
Recapito telefonico per eventuali comunicazioni:
Funzione rivestita:

E) Ulteriori soggetti coinvolti nel trattamento

Indicare i riferimenti di ulteriori soggetti coinvolti ed il ruolo svolto (contitolare, responsabile):

Denominazione: PA Digitale S.p.A.
Codice Fiscale/P.IVA: 06628860964 ☐ Soggetto privo di C.F./P.IVA italiana
Ruolo: Responsabile

Denominazione: WESTPOLE S.p.A
Codice Fiscale/P.IVA: 03705590580 ☐ Soggetto privo di C.F./P.IVA italiana
Ruolo: Responsabile

F) Informazioni sulla violazione

Riferimento interno della violazione:

1. Momento in cui è avvenuta la violazione

- ☐ a) Il
- ☒ b) Dal 08-12-2023 (la violazione è ancora in corso)
- ☐ c) Dal al
- ☐ d) In un tempo non ancora determinato
- ☐ e) In un tempo non determinabile

Ulteriori informazioni circa le date in cui è avvenuta la violazione

2. Modalità con la quale il titolare è venuto a conoscenza della violazione

- ☐ a) Rilevazione da parte del titolare
- ☒ b) Comunicazione da parte del responsabile del trattamento
- ☐ c) Segnalazione da parte di un interessato
- ☐ d) Segnalazione da parte di un soggetto esterno
- ☐ e) Notizie stampa
- ☐ f) Altro

3. Momento in cui il titolare è venuto a conoscenza della violazione

Data: 13-02-2023 Ora: 15 00

4. Motivi del ritardo (in caso di notifica oltre le 72 ore)

La presente notifica avviene entro le 72 ore

5. Natura della violazione

- ☐ a) Perdita di riservatezza
- ☐ b) Perdita di integrità
- ☒ c) Perdita di disponibilità

6. Causa della violazione

- ☐ a) Azione intenzionale interna
- ☐ b) Azione accidentale interna
- ☒ c) Azione intenzionale esterna
- ☐ d) Azione accidentale esterna
- ☐ e) Sconosciuta

- ☐ f) Non ancora determinata

7. Descrizione della violazione

Il responsabile del trattamento WESTPOLE S.p.A., Cloud Services Provider al quale mediante contratto di servizio PA Digitale S.p.A. ha affidato in hosting IaaS i propri servizi digitali, prevalentemente connessi alla fornitura di servizi di gestione digitali , notificava di aver subito un incidente di sicurezza, per atto deliberato di terzi ignoti. Segnalava, in particolare, che alle ore 11:00 AM del giorno 8 dicembre 2023 di aver rilevato "...la cifratura dell'intera infrastruttura informatica, all'interno dei dischi cifrati si rinveniva un file che identificava l'attaccante come gruppo LockBit che invitava a prendere contatti sulla darknet al fine di negoziare un pagamento per il rilascio delle chiavi di cifratura e relativo software per procedere al recupero". Come conseguenza, tutte le macchine virtuali e i backup, che inopinatamente erano tenuti in linea nello stesso ambiente di virtualizzazione, assieme anche al SIEM di monitoraggio, risultavano compromessi. La genericità dell'informativa fornita dal responsabile del trattamento non consente, allo stato, di fornire ulteriori dettagli

8. Descrizione dei sistemi, software, servizi e delle infrastrutture IT coinvolti nella violazione, con indicazione della loro ubicazione

Non si è a conoscenza nel dettaglio di tutta l'architettura di Westpole, ma vi è cognizione che le macchine virtuali, gli hypervisor VMWare, Citrix e tutta l'architettura di backup centralizzata, su entrambi i nodi gestiti da Westpole su Roma e Milano, risultavano totalmente compromessi. Westpole S.p.A., nella propria comunicazione, ha riferito di aver effettuato notifica a Codesta Autorità Garante in data 9 dicembre 2023.

9. Misure tecniche e organizzative, in essere al momento della violazione, adottate per garantire la sicurezza dei dati personali coinvolti

Come da contratto e da Livelli di Servizio stabiliti nell'accordo contrattuale e nella designazione di responsabile del trattamento, la società Westpole, già Hitachi Systems CBT, garantiva l'esistema di un sistema di gestione della sicurezza delle informazioni e dei servizi cloud, certificato secondo la norma ISO 27001:2022 e ISO 27017:2019, nonché una serie di presidi di segregazione, ridondanza, backup e monitoraggio, astrattamente idonei a preservare la disponibilità, integrità e riservatezza. Westpole S.p.A. risultava altresì fornitore certificato AgID di livello C dei servizi Cloud per la pubblica Amministrazione.

10. Categorie di interessati coinvolti nella violazione

- ☒ a) Dipendenti/Consulenti
- ☐ b) Utenti/Contraenti/Abbonati/Clienti (attuali o potenziali)
- ☐ c) Associati, soci, aderenti, simpatizzanti, sostenitori
- ☒ d) Soggetti che ricoprono cariche sociali
- ☐ e) Beneficiari o assistiti
- ☐ f) Pazienti
- ☐ g) Minori
- ☐ h) Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)
- ☐ i) Altro

- ☐ l) Categorie ancora non determinate

11. Numero (anche approssimativo) di interessati coinvolti nella violazione

- ☐ a) N. interessati
- ☒ b) Circa N.100 interessati
- ☐ c) Non determinabile
- ☐ d) Non ancora determinato

12. Categorie di dati personali oggetto di violazione

- ☒ a) Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale)
- ☒ b) Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
- ☒ c) Dati di accesso e di identificazione (username, password, customer ID, altro…)
- ☒ d) Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro…)
- ☐ e) Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro…)
- ☐ f) Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza
- ☐ g) Dati di profilazione
- ☒ h) Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro…)
- ☐ i) Dati di localizzazione
- ☐ l) Dati che rivelino l'origine razziale o etnici
- ☒ m) Dati relativi a opinioni politiche
- ☐ n) Dati relativi a convinzioni religiose o filosofiche
- ☒ o) Dati che rivelino l'appartenenza sindacale
- ☐ p) Dati relativi alla vita sessuale o all'orientamento sessuale
- ☒ q) Dati relativi alla salute
- ☐ r) Dati genetici
- ☐ s) Dati biometrici
- ☐ t) Altro

- ☐ u) Categorie ancora non determinate

13. Numero (anche approssimativo) di registrazioni dei dati personali oggetto di violazione

- ☐ a) N.
- ☐ b) Circa N.
- ☐ c) Non determinabile
- ☒ d) Non ancora determinato

14. Descrizione di dettaglio delle categorie di dati personali oggetto della violazione per ciascuna categoria di interessati

15. Allegati

☐ Intendo allegare un documento contenente ulteriori informazioni

G) Probabili conseguenze della violazione

1. Probabili conseguenze della violazione per gli interessati

1.1. In caso di perdita di riservatezza:

- ☐ a) I dati sono stati divulgati al di fuori di quanto previsto dall'informativa ovvero dalla disciplina di riferimento
- ☐ b) I dati possono essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati
- ☐ c) I dati possono essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito
- ☐ d) Altro

- ☐ e) In corso di valutazione

1.2. In caso di perdita di integrità:

- ☐ a) I dati sono stati modificati e resi inconsistenti
- ☐ b) I dati sono stati modificati mantenendo la consistenza
- ☐ c) Altro

- ☐ d) In corso di valutazione

1.3. In caso di perdita di disponibilità:

- ☒ a) Mancato accesso a servizi
- ☒ b) Malfunzionamento e difficoltà nell'utilizzo di servizi
- ☐ c) Altro

☐ d) In corso di valutazione

1.4. Ulteriori considerazioni sulle probabili conseguenze

2. Potenziale impatto per gli interessati

☒ a) Perdita del controllo dei dati personali
☐ b) Limitazione dei diritti
☐ c) Discriminazione
☒ d) Furto o usurpazione d'identità
☒ e) Frodi
☒ f) Perdite finanziarie
☐ g) Decifratura non autorizzata della pseudonimizzazione
☐ h) Pregiudizio alla reputazione
☐ i) Perdita di riservatezza dei dati personali protetti da segreto professionale
☒ l) Conoscenza da parte di terzi non autorizzati
☐ m) Qualsiasi altro danno economico o sociale significativo

☐ n) Non ancora definito

3. Gravità del potenziale impatto per gli interessati

☐ a) Trascurabile
☐ b) Bassa
☒ c) Media
☐ d) Alta
☐ e) Non ancora definita

l'indisponibilità del servizio si protrae per un tempo non superiore alla settimana nelle funzioni essenziali ; è possibile una indisponibilità più significativa per lo storico, con impatti ancora da misurare, da apprezzare non appena Westpole S.p.A. fornirà i dettagli

4. Allegati

☐ Intendo allegare un documento contenente ulteriori informazioni

H) Misure adottate a seguito della violazione

1. Misure tecniche e organizzative adottate (o di cui si propone l'adozione) per porre rimedio alla violazione e ridurne gli effetti negativi per gli interessati

E' stata richiesta la creazione di idoneo ambiente Iaas, garantito immune da compromissioni, al fine di ripristinare le macchine virtuali e i relativi applicativi, ricostruendo le basi dati. Sono state richieste informazioni di dettaglio alla società Westpole e si è in attesa di ottenere riscontro

2. Misure tecniche e organizzative adottate (o di cui si propone l'adozione) per prevenire simili violazioni future

Nel breve periodo l'obiettivo di PA Digitale S.p.A. è quello di ripristinare le funzionalità dei servizi e permettere agli utenti la piena accessibilità ai dati. PA Digitale ritiene necessario procedere alla strutturazione di diversa architettura verso altro fornitore, che permetta un maggiore livello di controllo sui parametri di disponibilità, integrità e riservatezza attesi

3. Allegati

☐ Intendo allegare un documento contenente ulteriori informazioni

I) Valutazione del rischio per gli interessati

1. Il titolare del trattamento ritiene che:

☐ a) la violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche

☒ b) la violazione non sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche

☐ c) siano necessari ulteriori elementi per effettuare la valutazione del rischio per i diritti e le libertà delle persone fisiche

Motivazioni

l'indisponibilità dei servizi risulta limitata e, stante la dichiarazione di Westpole S.p.A. secondo cui non vi sarebbe stata esfiltrazione dei dati, il ripristino delle funzionalità del processo risulta idoneo strumento per limitare gli impatti subiti dagli interessati.

2. Allegati

☐ Intendo allegare un documento contenente ulteriori informazioni

L) Comunicazione della violazione agli interessati

1. La violazione è stata comunicata direttamente agli interessati?

- ☐ a) Sì, è stata comunicata il
- ☒ b) No, sarà comunicata entro il 17-12-2023
- ☐ c) No, sono tuttora in corso le dovute valutazioni
- ☐ d) No, perché la violazione non è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
- ☐ e) No e non sarà comunicata perché:
  - ☐ e1) il titolare ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi (es. cifratura);

Descrivere le misure applicate

  - ☐ e2) il titolare ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

Descrivere le misure applicate

  - ☐ e3) detta comunicazione richiederebbe sforzi sproporzionati. Il titolare ha proceduto o procederà con una comunicazione pubblica o una misura simile, tramite la quale gli interessati sono o saranno informati con analoga efficacia.

Descrivere la modalità tramite la quale gli interessati sono stati informati

2. Numero di interessati a cui è stata comunicata la violazione

N. interessati

3. Canale utilizzato per la comunicazione agli interessati

- ☐ a) SMS
- ☐ b) Posta Cartacea
- ☐ c) Posta elettronica
- ☐ d) Altro

4. Contenuto della comunicazione agli interessati

Un significativo evento di sicurezza, che ha interessato il fornitore di servizi cloud Westpole S.p.A., ha causato l'indisponibilità dei sistemi della società PA Digitale a partire dalla prima mattina dell'8 dicembre 2023. In conseguenza dell'evento di cui si è venuti a conoscenza in data 13/12/2023, nonostante le rassicurazioni circa il fatto che al momento non risulti esfiltrazione di dati, si segnala la potenziale violazione di dati personali, trattati da PA Digitale nell'ambito del servizio di gestione economica e giuridica, relativo al personale dipendente, agli amministratori e ai professionisti destinatari di certificazione unica

5. Allegati

- ☐ Intendo allegare un documento contenente ulteriori informazioni

M) Altre informazioni

1. La violazione è stata notificata ad altri organismi di vigilanza o di controllo in virtù di ulteriori disposizioni normative?

☐ SI (indicare a quale organismo e in virtù di quale norma):

☒ NO

2. È stata effettuata la segnalazione all'autorità giudiziaria o di polizia?

☒ SI

☐ NO

Note

LA SEGNALAZIONE ALLE AUTORITA' PREPOSTE E' STATA FATTA DIRETTAMENTE DA WESTPOLE SPA

N) Informazioni relative a violazioni transfrontaliere

1. La violazione riguarda un trattamento transfrontaliero effettuato da un titolare stabilito all'interno dello Spazio Economico Europeo?

- ☐ a) SI
- ☒ b) No
- ☐ c) Sono tuttora in corso le dovute valutazioni