Istituzione “Cav. Paolo Sartori” – Comune di Valdastico (VI)

PIANO DI PROTEZIONE E MODELLO ORGANIZZATIVO PER LA PROTEZIONE DEI DATI PERSONALI

In applicazione del GDPR 2016/679 e del D.Lgs. 196/2003

Approvato con determinazione del Direttore n. 154 del 27.11.2020
Aggiornato con determinazione del Direttore n. 76 del 27.08.2025

Sommario

PARTE PRIMA: INTRODUZIONE

Articolo 1): PREMESSA DI CARATTERE NORMATIVO

Il presente Piano in materia di protezione dei dati personali (così detta “privacy”) è uno strumento di applicazione del vigente D.lgs. 30 giugno 2003, n. 196 (cosiddetto "Codice sulla privacy” come novellato dal recente D.lgs. 10 agosto 2018 n. 101) e, in particolare, del Regolamento Europeo n. 2016/679, nell'ambito dell'organizzazione dell’Istituzione “Cav. Paolo Sartori”.

A far data dal 25 maggio 2018 ha trovato diretta ed immediata applicazione, sul territorio nazionale, il nuovo Regolamento Europeo n. 2016/679 (così detto GDPR ossia “*General Data Protection Regulation*”) sulla privacy, approvato il 27 aprile 2016 e pubblicato sulla Gazzetta Ufficiale dell’Unione Europea il 4 maggio 2016.

Ciò ha comportato il superamento delle disposizioni legislative di cui al previgente Codice della privacy (D.lgs. 196/2003), così come delle norme regolamentari emanate negli anni dall’Autorità Garante per la protezione dei dati personali, nella misura in cui le norme nazionali risultino contrastanti o incompatibili con quelle europee.

Il principio cardine, di matrice anglosassone, introdotto dal nuovo Regolamento Europeo è quello della “responsabilizzazione” (*accountability* nell’accezione inglese) che pone in carico al Titolare del trattamento dei dati l’obbligo di attuare politiche adeguate in materia di protezione dei dati, con l’adozione di misure tecniche ed organizzative, anche certificate, che siano concretamente e sempre dimostrabili, oltre che conformi alle disposizioni europee (principio della “conformità” o *compliance* nell’accezione inglese); vi è quindi l’obbligo di porre in essere comportamenti proattivi, tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l’applicazione del Regolamento UE.

Nell’ottica del Legislatore europeo, quindi, in materia di privacy ciascun Titolare può scegliere autonomamente il modello organizzativo e gestionale che ritiene più adatto alla propria realtà e dotarsi delle misure di sicurezza che ritiene più efficaci in quanto Egli risponde delle proprie azioni e deve essere in grado, in qualsiasi momento, di darne conto verso l’esterno.

Il presente provvedimento si rende necessario per recepire, in un unico testo, i precetti normativi a maggior rilevanza, sia di carattere aziendale che nazionale in tema di trattamento dei dati personali, al fine darne collocazione sistematica nel contesto di questo ente.

Il presente provvedimento è sottoposto ad aggiornamento periodico, in linea con le novità normative, giurisprudenziali e con le pronunce del Garante per la protezione dei dati personali.

Articolo 2): PREMESSA DI CARATTERE ORGANIZZATIVO

Dall'esame della materia emerge come sia oramai imprescindibile un cambiamento di mentalità che porti alla piena tutela della privacy, da considerare non solo come un oneroso rispetto di adempimenti burocratici, ma, soprattutto, come garanzia, per il cittadino-utente che si rivolge alla struttura, di una completa riservatezza sotto il profilo sostanziale.

Il diritto alla privacy costituisce, anche secondo il Legislatore europeo, un vero e proprio diritto inviolabile dell’essere umano, che non si limita alla tutela della riservatezza o alla protezione dei dati, ma implica il pieno rispetto dei diritti e delle libertà fondamentali e della dignità del singolo individuo.

Per questi motivi, la “cultura della privacy” necessita di divenire un vero e proprio elemento cardine dell’organizzazione di questo ente, che deve impegnarsi perché la cultura di cui si tratta possa crescere e rafforzarsi, in quanto solo con la conoscenza minima dei principi fondamentali che stanno alla base della vigente normativa potranno essere adottati correttamente tutti gli adempimenti di carattere tecnico ed organizzativo nel trattamento dei dati di competenza.

PARTE SECONDA: DISPOSIZIONI GENERALI

Articolo 3): OGGETTO DEL PIANO

Il presente Piano disciplina, all'interno dell'Istituzione "Cav. Paolo Sartori", la tutela delle persone in ordine al trattamento dei dati personali, nel rispetto di quanto previsto dal Codice in materia di protezione dei dati personali (Decreto Legislativo del 30/06/2003 n. 196 e ss.mm.ii.) ed in conformità all'emanazione della normativa sovranazionale, il Regolamento UE n. 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.

Articolo 4): FINALITÀ DEL PIANO

L'Istituzione "Cav. Paolo Sartori" garantisce che il trattamento dei dati, a tutela delle persone fisiche, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

La protezione delle persone fisiche, con riguardo al trattamento dei dati personali, è un diritto fondamentale. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano (Articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione Europea).

Articolo 5): SENSIBILIZZAZIONE E FORMAZIONE

L'Istituzione "Cav. Paolo Sartori" sostiene e promuove, al suo interno, ogni strumento di sensibilizzazione che possa consolidare il pieno rispetto del diritto alla riservatezza e migliorare la qualità del servizio offerto all'utenza.

A tale riguardo, uno degli strumenti essenziali di sensibilizzazione, anche in materia di privacy, è l'attività formativa del personale e l'attività informativa diretta a tutti coloro che hanno rapporti con l'ente.

L'Istituzione "Cav. Paolo Sartori" organizza, nell'ambito della formazione continua e obbligatoria del personale, specifici interventi di formazione e di aggiornamento in materia di protezione dei dati personali, finalizzati alla conoscenza delle norme, alla prevenzione di fenomeni di abuso e illegalità nell'attuazione della normativa, all'adozione di idonei modelli di comportamento e procedure di trattamento, alla conoscenza delle misure di sicurezza per il trattamento e la conservazione dei dati, dei rischi individuati e dei modi per prevenire danni agli interessati.

La formazione in materia di prevenzione dei rischi di violazione dei dati personali viene integrata e coordinata con la formazione in materia di trasparenza e di accesso, con particolare riguardo ai rapporti tra protezione dei dati personali, trasparenza, accesso ai documenti amministrativi e accesso civico, semplice e generalizzato, nei diversi ambiti in cui opera l'Ente.

Articolo 6): DEFINIZIONI

Come stabilito dall'art. 4 del Regolamento Europeo n. 2016/679, ai fini di questo disciplinare si intende per:

a) «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può esser identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
b) «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione,

l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

c) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
d) «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
e) «pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
f) «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
g) «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;
h) «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
i) «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
j) «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;
k) «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;
l) «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
m) «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;
n) «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'art. 51 del Regolamento UE.

Quelle sopra riportate, di cui si è data evidenza, rappresentano le "definizioni" su cui ha inciso maggiormente il nuovo Regolamento europeo: per le altre "definizioni" si fa espresso rinvio al testo dell'art. 4 del Regolamento Europeo n. 2016/679 ed al D.lgs. 196/2003.

Articolo 7): PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI

Come stabilito dall'art. 5 del Regolamento Europeo n. 2016/679, i dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
b) 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 non è, conformemente all'art. 89, paragrafo 1 del Regolamento UE, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»). A tale proposito, il Regolamento UE ricalca i principi sostanziali di "necessità, pertinenza, indispensabilità e non eccedenza" (rispetto alle finalità del trattamento) contenuti nel D.lgs. 196/2003;
d) 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 («esattezza»);
e) 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, conformemente all'art. 89, paragrafo 1 del Regolamento UE, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
f) 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 («integrità e riservatezza»).

Articolo 8): CONDIZIONI DI LICEITÀ DEL TRATTAMENTO

Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il **consenso** al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è **necessario all'esecuzione di un contratto** di cui l'interessato è parte o all'esecuzione di **misure precontrattuali** adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un **obbligo legale** al quale è soggetto il titolare del trattamento;
d) il trattamento è necessario per la **salvaguardia degli interessi vitali** dell'interessato o di un'altra persona fisica;
e) il trattamento è necessario per l'**esecuzione di un compito di interesse pubblico** o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
f) il trattamento è necessario per il **perseguimento del legittimo interesse del titolare del trattamento o di terzi**, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore. Tale condizione non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

Articolo 9): CONDIZIONI PER IL CONSENSO

Per i trattamenti basati sul consenso dell'Interessato, il Titolare del trattamento deve essere in grado di dimostrare che l'Interessato abbia acconsentito al trattamento. In particolare, nel contesto di una dichiarazione scritta relativa a un'altra questione debbono esistere garanzie che assicurino che l'Interessato sia consapevole del fatto di prestare un consenso e della misura in

cui ciò avviene. Risulta opportuno prevedere una dichiarazione di consenso predisposta dal Titolare del trattamento in una forma comprensibile e facilmente accessibile, che usi un linguaggio semplice e chiaro e non contenga clausole abusive.

Il consenso non viene considerato liberamente prestato se l'Interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio.

Si presume che il consenso non sia stato liberamente prestato se non è possibile prestare un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso, o se l'esecuzione di un contratto, compresa la prestazione di un servizio, è subordinata al consenso sebbene esso non sia necessario per tale esecuzione.

Articolo 10): TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI

Premesso che l'Istituzione "Cav. Paolo Sartori" gestisce un centro servizi per anziani non autosufficienti e un centro diurno per anziani, il *core business* dell'ente è rappresentato dai servizi socio-assistenziali-sanitari svolti a favore degli ospiti. Al fine di svolgere tali servizi, l'ente necessita di trattare anche dati c.d. "particolari".

Come stabilito dall'art. 9 del Regolamento Europeo n. 2016/679, è vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Detta disposizione non si applica, secondo il Regolamento UE, quando incorrono alcune condizioni, riportate al summenzionato art. 9, tra le quali si evidenzia quella di cui alle lettere

- "h", ai sensi della quale "*il trattamento è necessario per finalità di […] diagnosi, assistenza o terapia sanitaria o sociale […]*"
- "g" ai sensi della quale "*il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri […]*".

A tal proposito l'art. 2-sexies del D.lgs. 196/2003 (come novellato dal D.lgs. 101/2018), prevede che "*si considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nelle seguenti materie: […]*

- *s) attività socio-assistenziale a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci;*
- *u) compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario;*
- *v) programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale*".

Si fa integrale rinvio all'art. 2-septies del D.lgs. 196/2003 (come novellato dal D.lgs. 101/2018) contenente specifiche disposizioni relative alle "misure di garanzia" per il trattamento dei dati genetici, biometrici e relativi alla salute.

Si richiama inoltre il provvedimento del Garante per la protezione dei dati personali n. 55 del 07.03.2019, ad oggetto "*Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario*", il quale specifica che "*Gli eventuali trattamenti attinenti, solo in senso lato, alla cura, ma non strettamente necessari, richiedono, quindi, anche se effettuati da professionisti della sanità, una distinta base giuridica da individuarsi, eventualmente, nel consenso dell'interessato o in un altro presupposto di liceità*".

Articolo 11): DOSSIER SANITARIO ELETTRONICO AZIENDALE

È implementato all'interno della struttura una Cartella Socio Sanitaria, la quale rappresenta un Dossier Sanitario Elettronico (abbreviato "D.S.E."), che raccoglie l'insieme dei dati personali

generati da eventi clinici presenti e trascorsi che riguardano il paziente, messi in condivisione logica al fine di documentarne la storia clinica e di offrirle un migliore processo di assistenza.

Per poter costituire il Dossier Sanitario Elettronico ed accedere a tutte le informazioni è necessario che il paziente rilasci il proprio consenso, dopo aver ricevuto l'apposita nota informativa. In ogni caso l'eventuale mancato consenso al trattamento dei dati personali mediante il Dossier sanitario non inciderà sulla possibilità di accedere alle cure mediche e alle attività di assistenza richieste.

Il Dossier sarà consultabile esclusivamente dal personale sanitario o socio-sanitario della struttura o da altro personale sanitario quando si renda necessaria una specifica consulenza specialistica concordata con l'interessato.

Il Dossier è implementato anche dalla fotografia del viso dell'ospite, in quanto ritenuto dato essenziale al fine di garantire la corretta somministrazione delle terapie e la corretta identificazione, anche in caso di turn over frequente del personale.

Si richiamano espressamente le "*Linee guida in materia di dossier sanitario*" predisposte dal Garante nell'allegato A alla deliberazione del 04.06.2015.

Articolo 12): TRATTAMENTO DEI DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI (DATI GIUDIZIARI)

Come stabilito dall'art. 10 del Regolamento Europeo n. 2016/679, "*il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza […] deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica*".

Posto quanto sopra, si fa integrale rinvio all'art. 2-octies del D.lgs. 196/2003 (come novellato dal D.lgs. 101/2018) dedicato al trattamento dei dati relativi a condanne penali e reati.

Articolo 13): CIRCOLAZIONE DEI DATI PERSONALI

Fatto salvo il rispetto di specifiche e puntuali disposizioni normative che lo vietino, l'Ente favorisce la circolazione all'interno dei propri uffici dei dati personali dei cittadini il cui trattamento sia necessario ai sensi degli articoli 6, 9 e 10 del GDPR. La circolazione, ove possibile, è assicurata mediante l'accessibilità diretta delle banche dati informative detenute da ciascun ufficio, previa creazione di appositi profili di utenza che tengano conto dei profili di autorizzazione conferiti. Forme similari di accessibilità sono garantite in favore di contitolari e responsabili del trattamento, limitatamente ai dati personali diversi da quelli contemplati dagli articoli 9 e 10 del GDPR.

Articolo 14): COMUNICAZIONE DI DATI VERSO L'ESTERNO

La comunicazione di dati personali da parte di un soggetto pubblico ad altro soggetto pubblico è ammessa quando è prevista da una norma di legge o regolamento e comunque quando è ritenuta necessaria per lo svolgimento di funzioni istituzionali, anche a seguito di un bilanciamento degli interessi in gioco.

Articolo 15): INFORMATIVA

Come stabilito dall'art. 13 del Regolamento Europeo n. 2016/679, in caso di raccolta presso l'Interessato di dati che lo riguardano, il Titolare del trattamento fornisce all'Interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:

a) l'identità e i dati di contatto del titolare del Trattamento e, ove applicabile, del suo rappresentante;

b) i dati di contatto del Data protection officer (DPO);
c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d) qualora il trattamento si basi sull'art. 6, paragrafo 1, lettera f) del Regolamento UE, i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione, nei termini previsti dal Regolamento UE.

In aggiunta alle informazioni di cui sopra, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:

a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
b) l'esistenza del diritto dell'Interessato di chiedere al Titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
c) qualora il trattamento sia basato sull'art. 6, paragrafo 1, lettera a), oppure sull'art. 9, paragrafo 2, lettera a) del Regolamento UE, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
d) il diritto di proporre reclamo a un'autorità di controllo;
e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
f) l'eventuale esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'art. 22, paragrafi 1 e 4 del Regolamento UE, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Ai fini dell'informativa, nell'ambito delle attività dell'Ente si identificano i seguenti ambiti:

a) prestazioni sanitarie, socio-assistenziali ed assimilate;
b) contratto di impegnativa economica;
c) rapporto di lavoro e assimilati;
d) rapporto di prestazione di servizi;
e) informazione generale pubblicata sul sito web;
f) breve informazione da porre in calce alle comunicazioni tramite e-mail.

Articolo 16): PERIODO DI CONSERVAZIONE

Per quanto concerne il periodo di conservazione dei dati personali raccolti da questo ente, i dati verranno conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello strettamente necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

A tale riguardo, il Titolare del trattamento provvederà ad approvare l'elenco della tipologia dei documenti con il rispettivo tempo di conservazione (limitato o illimitato); detto strumento permetterà di gestire in modo organizzato l'archivio aziendale, permettendo di conservare solo ciò che mantiene un rilievo giuridico o ha assunto un valore storico e di eliminare la documentazione non più necessaria.

Qualora il Titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'Interessato informazioni in merito a tale diversa finalità.

Articolo 17): SMALTIMENTO E DISTRUZIONE DEI DOCUMENTI

I principi elencati all'articolo 5 del Regolamento UE prevedono che anche la cancellazione (smaltimento e distruzione) dei documenti che contengono dati personali avvenga secondo il principio di responsabilizzazione del Titolare del trattamento. Tali documenti possono essere sia di tipo elettronico, conservati quindi su archivi informatici (cloud, hard disk, chiavette usb, cd-rom, dvd, …), sia di tipo cartaceo.

Per quanto riguarda la distruzione dei documenti elettronici si richiamano le istruzioni fornite dal Garante per la protezione dei dati personali, in particolare con il provvedimento "*Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali*" del 13 ottobre 2008. Prima di effettuare la distruzione dei supporti si rende comunque opportuno acquisire un parere dell'Amministratore di sistema, vista la particolare competenza tecnica necessaria al fine della distruzione sicura dei dati personali contenuti nei supporti digitali.

Per quanto riguarda la distruzione della documentazione cartacea, si considera conforme alla disciplina del Regolamento UE la distruzione effettuata mediante macchina distruggi documenti con livello di sicurezza di almeno P-4 secondo la normativa DIN 66399 (supporti dati con dati particolarmente sensibili e riservati, nonché dati personali che richiedono una maggiore protezione). È pertanto fatto obbligo a tutti i dipendenti di utilizzare tali apparecchiature per la distruzione di tutti i documenti cartacei contenenti dati personali.

Articolo 18): PRIVACY E OBBLIGHI DI PUBBLICAZIONE

Con il D.Lgs. n. 33/2013 il legislatore ha disciplinato in maniera organica i casi di pubblicità per finalità di trasparenza mediante inserzioni di dati, informazioni, atti e documenti sui siti web istituzionali degli enti. In particolare, gli obblighi di pubblicazione online di dati per finalità di "trasparenza" sono quelli indicati nel D.lgs. n. 33/2013 e nella normativa vigente in materia avente a oggetto le "*informazioni concernenti l'organizzazione e l'attività delle pubbliche amministrazioni, allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche*".

Accanto a questi obblighi di pubblicazione permangono altri obblighi di pubblicità online di dati, informazioni e documenti della PA – contenuti in specifiche disposizioni di settore diverse da quelle approvate in materia di trasparenza – come, fra l'altro, quelli volti a far conoscere l'azione amministrativa in relazione al rispetto dei principi di legittimità e correttezza, o quelli atti a garantire la pubblicità legale degli atti amministrativi (es.: pubblicità integrativa dell'efficacia, dichiarativa, notizia).

I principi e la disciplina di protezione dei dati personali devono essere rispettati anche nell'attività di pubblicazione di dati sul web per finalità di trasparenza. In particolare, la "diffusione" di dati personali da parte dei soggetti pubblici è ammessa unicamente quando la stessa è prevista da una specifica norma di legge o di regolamento. È, quindi, consentita la diffusione dei soli dati personali la cui inclusione in atti e documenti da pubblicare sia realmente necessaria e proporzionata alla finalità di trasparenza perseguita nel caso concreto (cd. "principio di pertinenza e non eccedenza"). Di conseguenza, i dati personali che esulano da tale finalità non devono essere inseriti negli atti e nei documenti oggetto di pubblicazione online. In caso contrario, occorre provvedere, comunque, all'oscuramento delle informazioni che risultano eccedenti o non pertinenti.

Si richiamano espressamente i seguenti provvedimenti del Garante per la protezione dei dati personali:

- "Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati" del 15.05.2014;
- "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico" del 14.06.2007;
- "Linee guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione di atti e documenti di enti locali" del 19.04.2007.

Tali provvedimenti indicano alcune azioni che le PA devono intraprendere al fine di bilanciare correttamente gli obblighi di trasparenza e il diritto alla riservatezza dei dati personali, in particolare:

- per rendere effettivamente "anonimi" i dati pubblicati online occorre oscurare del tutto il nominativo e le altre informazioni riferite all'interessato che ne possano consentire l'identificazione anche a posteriori;
- inserire nella sezione "Amministrazione trasparente" del proprio sito web un *alert* in cui si informi il pubblico che i dati personali pubblicati sono "*riutilizzabili solo alle condizioni previste dalla normativa vigente sul riuso dei dati pubblici (direttiva comunitaria 2003/98/CE e d. lgs. 36/2006 di recepimento della stessa), in termini compatibili con gli scopi per i quali sono stati raccolti e registrati, e nel rispetto della normativa in materia di protezione dei dati personali*";
- nella pubblicazione dei curricula, provvedere ad oscurare tutti i dati eccedenti le finalità di trasparenza; possono essere ritenute pertinenti le informazioni riguardanti i titoli di studio e professionali, le esperienze lavorative, conoscenze linguistiche o nell'uso di tecnologie; non devono invece essere oggetto di pubblicazioni dati personali eccedenti quali i recapiti personali ed il codice fiscale;
- ove la normativa imponga la pubblicazione concernenti corrispettivi e compensi, risulta proporzionato indicare il compenso complessivo percepito, ma non la versione integrale di documenti o eventuali dichiarazioni fiscali.

Inoltre, per quanto riguarda i concorsi e le selezioni, possono essere pubblicati dolo i dati pertinenti e non eccedenti ai fini del corretto espletamento delle procedure, anche tenuto conto dell'aggiornamento al DPR 487/1994 avvenuto con DPR 82/2023, quindi nello specifico è lecito pubblicare i dati personali secondo le indicazioni della seguente tabella:

Documento contenente dati personali	**Identificativo personale**	**Dati pubblicati**	**Pubblicazione sul portale InpA**	**Pubblicazione sul sito istituzionale dell'ente**
Convocazione alla prova successiva	Codici identificativi rilasciati dal portale InpA	Ammissione e non ammissione	Sì	No
Esiti delle prove intermedie	Codici identificativi rilasciati dal portale InpA	Punteggio parziale conseguito	Sì	Sì, all'albo pretorio online per 10 giorni
Graduatoria finale	Vincitori: Nominativi in chiaro - Idonei: Codici identificativi rilasciati dal portale InpA	Posizione in graduatoria e punteggio totale conseguito	Sì	Sì, nella sezione Amministrazione Trasparente per 5 anni

Per quanto riguarda gli atti di organizzazione degli uffici contenenti dati personali, appare opportuno oscurare tutti i dati riferiti al dipendente interessato rendendo anonimo il dato nei documenti oggetto di pubblicazione online. L'atto completo di tutte le informazioni sarà invece trattato dall'ufficio preposto.

Fermo restando che i presupposti, le modalità ed i limiti per l'esercizio del diritto di accesso ai documenti amministrativi e del diritto di accesso civico, semplice e generalizzato e la relativa

tutela giurisdizionale, così come gli obblighi di pubblicità e pubblicazione, restano disciplinati dalla normativa di settore - gli uffici dovranno interpretare la vigente normativa in materia di trasparenza ed accesso in modo da garantire la più rigorosa tutela dei dati personali degli interessati, anche tenendo in considerazione le motivazioni addotte dal soggetto controinteressato.

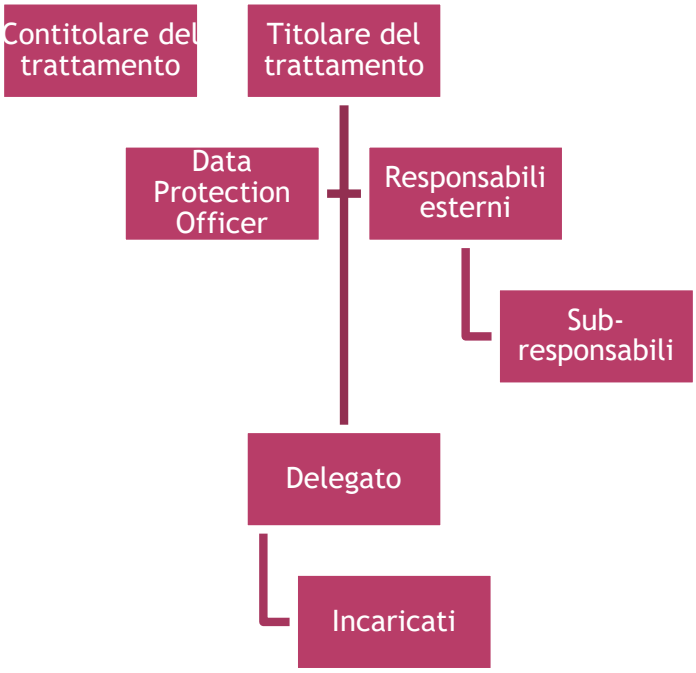
PARTE QUARTA: TITOLARE DEL TRATTAMENTO E ALTRE FIGURE

Articolo 19): ASSETTO ORGANIZZATIVO PRIVACY

Il D.lgs. 196/2003, come novellato dal D.lgs. 101/2018 di armonizzazione del Codice italiano della privacy alle novità del GDPR Europeo n. 2016/679, stabilisce, all'articolo 2-quaterdecies, comma 1, che il Titolare può "*prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la propria autorità*".

L'Istituzione "Cav. Paolo Sartori", in qualità di Titolare del trattamento di dati personali, è tenuta a delineare al proprio interno un'adeguata ed efficace articolazione delle responsabilità al fine di assicurare il rispetto delle disposizioni vigenti in materia, e ciò sulla base del principio europeo di *accountability*, che prevede il coinvolgimento e la responsabilizzazione, ad ogni livello, delle strutture dell'azienda nel percorso di adeguamento ai precetti europei.

Ai fini del rispetto del principio di accountability si definisce un "assetto organizzativo privacy", raffigurabile come indicato di seguito:



Articolo 20): TITOLARE DEL TRATTAMENTO

L'art. 4 n. 7 del GDPR precisa che il titolare del trattamento (interpretando la norma rispetto alla pubblica amministrazione) è "*l'autorità pubblica*" che "*determina le finalità e i mezzi del trattamento di dati personali*". Il concetto di Titolare del trattamento serve a determinare in primissimo luogo chi risponde dell'osservanza delle norme relative alla protezione dei dati.

Competenze e responsabilità

Le competenze e le responsabilità che il GDPR assegna al Titolare del trattamento possono così essere riassunte:

- determinare le finalità ed i mezzi del trattamento dei dati personali: in considerazione del carattere pubblico che contraddistingue questa Amministrazione, le finalità sono determinate e circoscritte in quelle necessarie a garantire il corretto svolgimento delle funzioni istituzionali e dei compiti di interesse pubblico (art. 4);
- mettere in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR (c.d. accountability) (art. 24);
- garantire che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali non tratti tali dati se non è adeguatamente istruito in tal senso (artt. 29 e 32);
- individuare i responsabili del trattamento, controllarne e garantirne l'operato (art. 28);
- agevolare l'esercizio dei diritti dell'interessato (art. 12) e fornire agli interessati le informazioni previste dal GDPR (art. 13);
- designare il Responsabile della protezione dei dati (art. 37) ponendolo in grado di svolgere adeguatamente l'attività (art. 38);
- istituire e tenere aggiornato un registro delle attività di trattamento svolte sotto la propria responsabilità (art. 30);
- effettuare, prima di procedere al trattamento, una valutazione dell'impatto sulla protezione dei dati personali (art. 35);
- comunicare all'autorità di controllo (art. 33) ed all'interessato (art. 34) eventuali violazioni dei dati;
- ricevere ed osservare provvedimenti, notifiche e ingiunzioni dell'autorità di controllo (art. 58);
- rispondere per il danno cagionato dal trattamento che violi il GDPR (art. 82);
- rispondere delle violazioni amministrative ai sensi del GDPR (art. 83).

Alla luce del testo normativo e delle interpretazioni correnti, si ritiene che Titolare sia l'Istituzione nel suo complesso, autonoma rispetto a quella del Comune di Valdastico, in quanto la legislazione nazionale gli ha affidato il compito di raccogliere e trattare certi dati personali. Le competenze e le responsabilità quali delineate dal GDPR e dalla normativa nazionale in tema di protezione dei dati personali sono attribuite agli organi dell'ente in relazione alle funzioni agli stessi assegnati dallo statuto. Tale ripartizione è così intesa da questa Amministrazione:

A. al **Consiglio di Amministrazione** sono assegnate:
   a) le competenze di tipo regolatorio o programmatorio generale in materia di riservatezza dei dati;

B. al **Presidente** spettano i seguenti compiti:
   a) vigilare sulla corretta informazione e sull'esercizio dei diritti degli interessati;
   b) disporre l'adozione dei provvedimenti imposti dal Garante, per quanto di competenza;
   c) collaborare con il Responsabile della protezione dei dati personali al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;

C. al **Direttore** spettano i seguenti compiti (con elencazione meramente esemplificativa):
   a) approvare e modificare il "Piano di protezione e modello organizzativo per la protezione dei dati personali";
   b) attribuire le nomine e le designazioni rilevanti in materia di protezione dei dati personali, con riferimento in particolare al Responsabile della protezione dei dati, ai soggetti designati con funzioni di coordinamento e al referente;
   c) verificare la legittimità dei trattamenti di dati personali effettuati dalla struttura;

d) disporre le modifiche necessarie al trattamento perché lo stesso sia conforme alla normativa vigente ovvero disporre la cessazione di qualsiasi trattamento effettuato in violazione alla stessa;
e) implementare una valutazione dei rischi legata al trattamento dei dati personali;
f) adottare soluzioni di *privacy by design* e *by default*;
g) aggiornare costantemente il registro delle attività di trattamento;
h) implementare il registro dei *data-breach* qualora necessario;
i) garantire la corretta informazione e l'esercizio dei diritti degli interessati;
j) individuare e sottoscrivere il contratto con i responsabili del trattamento, ai sensi dell'art. 28, comma 3, del Regolamento UE 2016/679;
k) individuare i soggetti Incaricati a compiere operazioni di trattamento (di seguito anche "Incaricati al trattamento") fornendo agli stessi istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite;
l) autorizzare altresì anche eventuali collaboratori "esterni" (persone fisiche), a prescindere dal rapporto contrattuale intrattenuto con l'Amministrazione (ad es. stagisti, tirocinanti, singoli volontari, …) purché non dotati di potere decisionale autonomo e stabilmente presenti in struttura per un dato periodo;
m) disporre l'adozione dei provvedimenti imposti dal Garante, per quanto di competenza;
n) collaborare con il Responsabile della protezione dei dati personali al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;
o) garantire al Responsabile della protezione dei dati personali ed al personale designato Amministratore di Sistema i necessari permessi di accesso ai dati ed ai sistemi per l'effettuazione delle verifiche di sicurezza, anche a seguito di incidenti di sicurezza;
p) la preventiva valutazione d'impatto ai sensi dell'art. 35 del Regolamento, nei casi in cui un trattamento, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche e le eventuali consultazioni con il Garante ai sensi dell'art. 36 del Regolamento;
q) gestire la procedura in relazione alle violazioni di dati personali, curando la notifica all'Autorità di controllo e l'eventuale comunicazione agli interessati.

Il Direttore può delegare uno o più compiti ad altro personale specificatamente individuato.

Articolo 21): CONTITOLARE DEL TRATTAMENTO

Come stabilito dall'art. 26 del Regolamento Europeo n. 2016/679, allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono Contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal Regolamento UE, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni.

Tale accordo può designare un punto di contatto per gli interessati e riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli Interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'Interessato.

Indipendentemente dalle disposizioni dell'accordo anzidetto, l'Interessato può esercitare i propri diritti ai sensi del Regolamento UE nei confronti di e contro ciascun Titolare del trattamento.

Articolo 22): DELEGATO ALLA GESTIONE DELLE ATTIVITÀ DI TRATTAMENTO DEI DATI

In considerazione della complessità e della molteplicità delle funzioni istituzionali dell'Amministrazione, può essere introdotta la figura "intermedia" del "Delegato alla gestione delle attività di trattamento dei dati".

Tale figura provvede ad eseguire i compiti eventualmente delegati dal Direttore in qualità di Titolare del trattamento.

Articolo 23): RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI

Il concetto di "Responsabile del trattamento" riveste un ruolo importante nel contesto della riservatezza e sicurezza dei trattamenti poiché serve ad individuare le responsabilità di coloro che si occupano più da vicino dell'elaborazione dei dati personali, sotto l'autorità diretta del Titolare del trattamento o per suo conto.

L'esistenza di un Responsabile del trattamento dipende da una decisione presa dal Titolare. Quest'ultimo può decidere di trattare i dati all'interno della propria organizzazione, ad esempio attraverso collaboratori autorizzati a trattare i dati sotto la sua diretta autorità, o di delegare tutte o una parte delle attività di trattamento a un'organizzazione esterna.

A norma dell'articolo 28, paragrafo 1 del GDPR "*Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato*".

Per poter agire come Responsabile del trattamento occorrono quindi due requisiti: essere una persona giuridica distinta dal Titolare ed elaborare i dati personali per conto di quest'ultimo. La liceità dell'attività di trattamento dei dati da parte del Responsabile è determinata dal mandato ricevuto dal Titolare del trattamento. Se va al di là del proprio mandato e se acquisisce un ruolo rilevante nella determinazione delle finalità o degli aspetti fondamentali dei mezzi del trattamento, il Responsabile diventa (con)Titolare.

Si deve tuttavia prendere atto del fatto che esistano situazioni in cui la relazione tra l'Ente ed un altro soggetto, pubblico o privato, possa generare dei dubbi in merito alla corretta qualificazione del ruolo soggettivo rivestito (Titolare o Responsabile). Con riferimento a tali fattispecie, questo Ente adotta il criterio della valutazione delle circostanze di fatto, suggerito dal Gruppo ex art. 29 nel Parere 1-2010 (WP 169). Il paragrafo 3 dell'articolo 28 del GDPR prevede che "*I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento*"; il paragrafo 9, da ultimo, prevede che "*Il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 è stipulato in forma scritta, anche in formato elettronico*".

Spetta al Direttore identificare i responsabili e gli eventuali sub-responsabili, e sottoscrivere i contratti/appendici contrattuali per il trattamento dei dati, avendo cura di tenere costantemente aggiornata la relativa documentazione nonché acquisire dai responsabili e dagli eventuali sub responsabili l'elenco nominativo delle persone fisiche che, presso gli stessi, risultano autorizzate al trattamento dei dati ed a compiere le relative operazioni. Il Direttore ha il dovere di verificare che il soggetto esterno osservi le predette prescrizioni; l'Amministratore del sistema informatico verifica che siano osservate le norme riferite all'attuazione delle misure minime di sicurezza. La periodicità delle predette verifiche, previste nel provvedimento o contratto di affidamento, è determinata in funzione della natura dei dati, della probabile gravità dei rischi, dei mezzi da utilizzare per il trattamento e della durata dell'affidamento. Le verifiche e i risultati delle stesse sono registrate in appositi distinti verbali, sottoscritti, in duplice originale, dal Responsabile del trattamento e dal soggetto che svolge ciascuna verifica.

Articolo 24): SUB-RESPONSABILE DEL TRATTAMENTO DEI DATI

Il Responsabile del trattamento non ricorre a un altro Responsabile senza previa autorizzazione scritta, specifica o generale, del Titolare del trattamento.

Nel caso di autorizzazione scritta generale, il Responsabile del trattamento informa il Titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri Responsabili del trattamento, dando così al Titolare del trattamento l'opportunità di opporsi a tali modifiche.

Quando un Responsabile del trattamento ricorre a un altro Responsabile del trattamento per l'esecuzione di specifiche attività, su tale altro Responsabile sono imposti, mediante un contratto o un altro atto giuridico, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il Titolare del trattamento e il Responsabile del trattamento, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate.

Qualora l'altro Responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile iniziale conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro Responsabile.

Articolo 25): INCARICATO (INTERNO ED ESTERNO) AL TRATTAMENTO DEI DATI

Il D.lgs. 196/2003, come novellato dal D.lgs. 101/2018 stabilisce, all'art. 2-quaterdecies, comma 2, che il Titolare "*individua le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta*".

Ciò detto, sulla base del principio europeo di *accountability*, il Titolare del trattamento provvede ad individuare le persone "incaricate al trattamento dei dati" ai sensi dell'art. 2-quaterdecies, comma 2, del D.lgs. 196/2013.

Al momento dell'ingresso in servizio è fornita, a cura dell'ufficio di gestione delle risorse umane, ad ogni dipendente (oltre che ad ogni collaboratore esterno) una specifica comunicazione in materia di privacy, con la quale detti soggetti (dipendenti e non dipendenti) vengono nominati quali "incaricati al trattamento dei dati" ai sensi del D.lgs. 196/2003 e del Regolamento UE 2016/679, impartendo loro anche le opportune "istruzioni operative".

Al fine di dare evidenza di quale tipologia di dati possono trattare le varie figure (interne/esterne), si espone una matrice generale per il trattamento dei dati:

	DATI COMUNI OSPITI (oltre ai congiunti, rappresentanti legali e familiari)	DATI PARTICOLARI DEGLI OSPITI (relativi alla salute)	DATI COMUNI DEI DIPENDENTI (e del nucleo familiare)	DATI PARTICOLARI DEI DIPENDENTI (e del nucleo familiare)	DATI COMUNI DEI COLLABORATORI ESTERNI E DEI FORNITORI
Direttore					
Coordinatore dei Servizi			(solo dati di contatto)	(solo limitazioni alle mansioni)	
Preposti ai sensi del D.Lgs. 81/2008				(solo limitazioni alle mansioni)	
Personale amministrativo					
Assistente sociale					
Infermieri			(solo dati di contatto)		
Operatori socio-assistenziali					

Educatore					
Fisioterapista - Logopedista					
Medico					
Psicologo					
Manutentore	(solo dati identificativi)				
Personale delle funzioni ausiliarie (lavanderia, pulizie, cucina)	(solo dati identificativi)				
Volontari	(solo dati identificativi)				

Al fine di dare completa informazione e formazione agli Incaricati che utilizzano i sistemi informatici, è predisposto un apposito "Disciplinare sulle misure di sicurezza degli strumenti informatici", di cui all'Allegato A, che viene consegnato a cura dell'ufficio di gestione delle risorse umane a tutti gli Incaricati destinatari, anche tramite pubblicazione nel portale per la gestione del personale.

Articolo 26): DATA PROTECTION OFFICER

Il Regolamento Europeo impone alle autorità ed agli organismi pubblici la nomina del Data Protection Officer (in italiano: Responsabile della protezione dei dati o 'RPD'), nei termini di cui agli artt. 37, 38 e 39 del Regolamento medesimo.

Il DPO deve presentare caratteristiche di indipendenza ed autorevolezza, oltre che competenze manageriali. Non deve, inoltre, essere in conflitto di interessi in quanto il Regolamento UE vieta di nominare DPO anche chi, solo in astratto, possa potenzialmente trovarsi in conflitto di interessi.

Si tratta di una figura dirigenziale, di alta professionalità, a metà tra il consulente ed il revisore e non dovrebbe ricoprire ruoli gestionali rispetto all'attività della Pubblica Amministrazione.

Ai sensi dell'art. 39 del Regolamento UE, i suoi compiti sono:

a) informare e fornire consulenza al Titolare del trattamento, nonché ai dipendenti che eseguono il trattamento, in merito agli obblighi derivanti dal Regolamento UE nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b) sorvegliare l'osservanza del Regolamento UE, di altre disposizioni dell'Unione o degli Stati membri 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 la stessa per questioni connesse al trattamento, tra cui la consultazione preventiva, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Ai sensi dell'art. 37 del Regolamento UE, il DPO deve:

a) possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali, anche in termini di misure tecniche e organizzative o di misure atte a garantire la sicurezza dei dati. Non sono richieste attestazioni formali o l'iscrizione ad appositi albi professionali, anche se la partecipazione a master e corsi di studio/professionali può

rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenze;

b) adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse. In linea di principio, ciò significa che il DPO non può essere un soggetto che ricopre ruoli gestionali e che decide sulle finalità o sugli strumenti del trattamento di dati personali;
c) operare alle dipendenze del Titolare oppure sulla base di un contratto di servizio (DPO esterno);
d) disporre di risorse umane e finanziarie, messe a disposizione dal Titolare, per adempiere ai suoi scopi.

Il Regolamento UE prevede la pubblicazione sul sito istituzionale dell'Ente dei "dati di contatto" del DPO; i medesimi dati devono essere inseriti anche nell'informativa aziendale sul trattamento dei dati, così che il DPO sia agevolmente contattabile.

Articolo 27): AMMINISTRATORE DI SISTEMA (AdS)

L'Amministratore di sistema, individuato dal Titolare del trattamento, sovraintende alla gestione e alla manutenzione delle banche dati e, nel suo complesso, al sistema informatico di cui è dotato l'Ente.

La nomina dell'Amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati e in tema di sicurezza. La designazione dell'Amministratore di sistema è individuale e deve recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

In ambito di protezione dei dati personali, l'Amministratore di sistema propone al Titolare del trattamento un documento di valutazione del rischio informatico, da aggiornare con cadenza annuale.

Nel rispetto della normativa in materia di protezione dei dati e della sicurezza, l'Amministratore di sistema deve adottare sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici. Le registrazioni (*access log*) devono essere complete, inalterabili, verificabili nella loro integrità, e adeguate al raggiungimento dello scopo di verifica per cui sono richieste. Le registrazioni devono comprendere il riferimento temporale e la descrizione dell'evento che le ha generate e devono essere conservate per un periodo congruo, non inferiore ai sei mesi.

L'Amministratore di sistema applica le disposizioni impartite dal Garante in materia di misure e accorgimenti effettuati con strumenti elettronici.

Articolo 28): REFERENTE PER LA PROTEZIONE DEI DATI PERSONALI

Ai sensi dell'articolo 38 del GDPR, il Titolare ha l'obbligo di assicurarsi che "*il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali*"; il Titolare inoltre sostiene "*il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica*".

In caso di nomina di un DPO esterno all'organizzazione, si ravvisa dunque la necessità - nell'ottica di un adeguamento in qualità ai nuovi istituti previsti dal GDPR, alla luce del contesto, della natura e della complessità dei trattamenti effettuati - di individuare uno o più dipendenti interni all'ente cui assegnare il compito di "Referente" al fine di supportare l'attività del Responsabile della Protezione dei dati personali (DPO), nelle seguenti attività:

a) Informazione e consulenza al Titolare del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR. Tale attività comporta il supporto nella redazione di pareri, note, circolari, policy, newsletter con

segnalazione delle novità normative e giurisprudenziali in materia di protezione dei dati personali e delle migliori *best practice* in materia di analisi e valutazione dei rischi.

b) Sorveglianza dell'osservanza del GDPR, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo.

c) Fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del GDPR. Tale attività comporta un supporto nelle interviste a responsabili di settore, ICT, partecipazione a riunioni, analisi di documentazione tecnica, studio degli ambienti di prova dei software e della relativa documentazione tecnica.

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 prevista dall'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione. Tale attività comporta un supporto nel riscontro alle richieste di informazioni inviate dal Garante e nelle eventuali ispezioni dell'Autorità.

Il Referente è tenuto al segreto od alla riservatezza in merito all'adempimento dei propri compiti e alle informazioni e dati di cui potrebbe venire a conoscenza nell'esercizio delle proprie funzioni. Egli è inoltre tenuto a segnalare al DPO ogni possibile situazione di conflitto di interesse, anche potenziale rispetto ai propri compiti, incarichi e funzioni.

Ove i compiti assegnati al Referente vengano svolti in modo collettivo da parte di un team, dovrà essere designato un soggetto coordinatore.

PARTE QUINTA: SICUREZZA DEI DATI PERSONALI E MISURE DI SICUREZZA

Articolo 29): PROTEZIONE DEI DATI

Come esposto nel considerando 78, la tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del Regolamento UE.

L'art. 25 del Regolamento Europeo n. 2016/679 introduce il criterio sintetizzato dall'espressione inglese "*data protection by default and by design*", ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili al fine di soddisfare i requisiti del regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

Tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, pseudonimizzare i dati personali il più presto possibile, offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali, consentire all'Interessato di controllare il trattamento dei dati e consentire al Titolare del trattamento di creare e migliorare le caratteristiche di sicurezza.

Articolo 30): REGISTRO ELETTRONICO DELLE ATTIVITÀ DI TRATTAMENTO

Tutti i Titolari e i Responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti che non effettuano trattamenti a rischio devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30 del Regolamento UE.

Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un soggetto pubblico, indispensabile per ogni valutazione e analisi del rischio.

Il Registro deve essere esibito su richiesta del Garante.

Il registro delle attività di trattamento costituisce uno dei principali elementi di *accountability* del Titolare, in quanto strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, indispensabile per ogni attività di valutazione o analisi del rischio e dunque preliminare rispetto a tali attività.

Il registro delle attività di trattamento è esposto nell'Allegato B).

Il registro può essere sottoposto a revisioni da parte del Direttore senza la necessità di approvazione con specifico provvedimento, data la sua natura estremamente dinamica e soggetta a frequenti aggiornamenti, acquisendo come data certa la marcatura di protocollo.

Articolo 31): VALUTAZIONE E GESTIONE DEI RISCHI

La valutazione dei rischi è necessaria, tra l'altro:

a) per determinare l'adeguatezza delle misure di sicurezza a protezione dei trattamenti di dati personali;
b) per determinare la necessità di una valutazione d'impatto sui trattamenti e nella valutazione d'impatto stessa;
c) per determinare la necessità di segnalazione di una violazione di dati personali all'autorità di controllo.

La normativa non indica orientamenti specifici per la messa in atto di opportune misure e per dimostrare la conformità da parte del Titolare del trattamento in particolare per quanto riguarda l'individuazione del rischio connesso al trattamento, la sua valutazione in termini gravità e probabilità, e l'individuazione di migliori prassi per attenuare il rischio: le scelte in materia di gestione del rischio sono responsabilità del Titolare del trattamento, secondo il principio di responsabilizzazione.

Articolo 32): VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

La valutazione d'impatto sulla protezione dei dati (DPIA: *data protection impact assessment*, nell'accezione inglese) è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli.

La DPIA è uno strumento importante per la responsabilizzazione in quanto sostiene il Titolare non soltanto nel rispettare i requisiti del GDPR, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del medesimo GDPR.

La DPIA sulla protezione dei dati personali deve essere realizzata, prima di procedere al trattamento, dal Titolare del trattamento quando un tipo di trattamento, considerata la natura, il contesto, le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Vengono qui espressamente richiamate le "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento possa presentare un rischio elevato*", predisposte dal Gruppo di lavoro WP29 in data 04.10.2017. In particolare, fra i trattamenti che possono presentare un rischio elevato, viene individuato il criterio dei dati relativi a interessati vulnerabili, nei casi dove sia possibile individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del Titolare del trattamento. Nei trattamenti di questo ente tali squilibri si possono identificare nei confronti degli ospiti (persone anziane solitamente non autosufficienti) e dei dipendenti.

Tuttavia le linee guida prevedono l'obbligo di procedere con la valutazione d'impatto qualora il trattamento soddisfi ulteriori criteri (almeno due) tra quelli elencati.

Considerato che il *core business* dell'Ente è la gestione dell'ospite anziano in stato di bisogno, e che vengono costantemente trattati dati personali sia di tipo comune che di tipo particolare, il Titolare del trattamento può prevedere di realizzare una valutazione di impatto su tale trattamento.

Articolo 33): VIOLAZIONE DEI DATI PERSONALI

Per violazione dei dati personali (in seguito "*data breach*") si intende la violazione di sicurezza che comporti, accidentalmente od in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dall'Ente (tale indicazione operativa pertanto si applica a tutti gli archivi/documenti cartacei ed a tutti i sistemi, anche informativi sui quali siano conservati i dati personali degli interessati, quali ospiti, dipendenti, fornitori, soggetti terzi, ecc.).

La segnalazione di un possibile *Data Breach* può provenire dall'esterno (persone di riferimento degli ospiti, familiari, fornitori esterni, enti istituzionali ecc.) o dall'interno, durante il normale svolgimento dell'attività lavorativa.

Colui il quale riceve la segnalazione dall'esterno o che rileva dall'interno l'evento anomalo di violazione di dati personali, deve darne immediata notizia al Direttore compilando ed inviando il "Modello di potenziale violazione di dati personali" (Allegato C).

Il Direttore, con la collaborazione di eventuali delegati, deve:

a) adottare le misure di sicurezza informatiche e/o organizzative per porre rimedio o attenuare i possibili effetti negativi della violazione dei dati personali e, contestualmente, informa immediatamente il DPO per una valutazione condivisa;
b) condurre e documentare un'indagine corretta e imparziale sull'evento (aspetti organizzativi, informatici, legali, ecc;
c) riferire i risultati dell'indagine informando il DPO.

Il DPO, ricevuti i risultati dell'indagine, analizza l'accaduto e formula un parere in merito all'evento, esprimendo la propria valutazione, non vincolante. Lo invia quindi al Direttore.

Notifica all'Autorità di controllo

Il Direttore, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione all'Autorità di controllo. La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo. Qualora la notifica effettuata nelle 72 ore non sia completa è possibile integrarla in una o più fasi successive (ad es. nel caso di violazioni complesse per le quali occorrono indagini approfondite) corredandola con i motivi (analogamente come in caso di notifica in ritardo). Nel caso in cui la scoperta della violazione non sia contestuale al verificarsi dell'evento che l'ha generata, devono essere indicate nella comunicazione le motivazioni che non hanno consentito l'immediata rilevazione dell'evento stesso e le misure adottate o che si intende adottare affinché ciò non si ripeta in futuro.

La notifica sarà effettuata utilizzando il servizio messo a disposizione dal Garante per la protezione dei dati personali all'indirizzo https://servizi.gpdp.it/databreach/s/, così come definita dal provvedimento della medesima autorità del 27.05.2021.

Il Responsabile del trattamento eventualmente coinvolto deve:

a) informare il Direttore tempestivamente ed in ogni caso entro e non oltre 72 ore dalla scoperta dell'evento, tramite PEC, di essere venuto a conoscenza di una violazione e fornire tutti i dettagli della violazione subita, in particolare una descrizione della natura della violazione dei dati personali, le categorie e il numero approssimativo di interessati coinvolti, nonché le categorie e il numero approssimativo di registrazioni dei dati in questione, l'impatto della violazione dei dati personali sull'Ente e sugli Interessati coinvolti e le misure adottate per mitigare i rischi;
b) fornire assistenza per far fronte alla violazione ed alle sue conseguenze soprattutto in capo agli Interessati coinvolti. Il Direttore si attiverà per mitigare gli effetti delle violazioni, proponendo tempestive azioni correttive. Tali misure sono richieste al fine di garantire un livello di sicurezza adeguato al rischio correlato al trattamento eseguito. Risulta opportuno e di particolare importanza che tutti gli atti di designazione a Responsabile del trattamento contengano una espressa previsione circa la necessità di

informare l'Ente, senza ingiustificato ritardo, in caso di avvenuta conoscenza di una violazione di dati personali, anche solo probabile o possibile.

I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del RGPD, sono i seguenti:

a) danni fisici, materiali o immateriali alle persone fisiche;
b) perdita del controllo dei dati personali;
c) limitazione dei diritti, discriminazione;
d) furto o usurpazione d'identità;
e) perdite finanziarie, danno economico o sociale;
f) decifratura non autorizzata della pseudonimizzazione;
g) pregiudizio alla reputazione;
h) perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).

Notifica agli Interessati

Ove il Direttore ritenga che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata sia elevato, deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi. Prima di procedere alla comunicazione della violazione ai soggetti interessati il testo della comunicazione, le modalità di notifica e le evidenze che attestano il reale livello di pregiudizio, dovranno essere concordate con il DPO. Nel caso in cui la comunicazione dovesse pregiudicare lo svolgimento delle verifiche sull'evento *Data Breach*, il Direttore può chiedere all'Autorità di controllo l'autorizzazione a ritardare la citata comunicazione per il tempo necessario all'espletamento di tali verifiche.

La probabilità e la gravità del rischio, per i diritti e le libertà dell'interessato, dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato.

A tal fine l'Ente individua nel documento "*Recommendations for a methodology of the assessment of severity of personal data breaches*" dell'ENISA la metodologia da utilizzare per tale valutazione. Tali raccomandazioni sono disponibili all'indirizzo: https://www.enisa.europa.eu/publications/dbn-severity.

La traduzione in italiano è allegata al presente documento all'Allegato D.

Registro dei Data Breach

Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio.

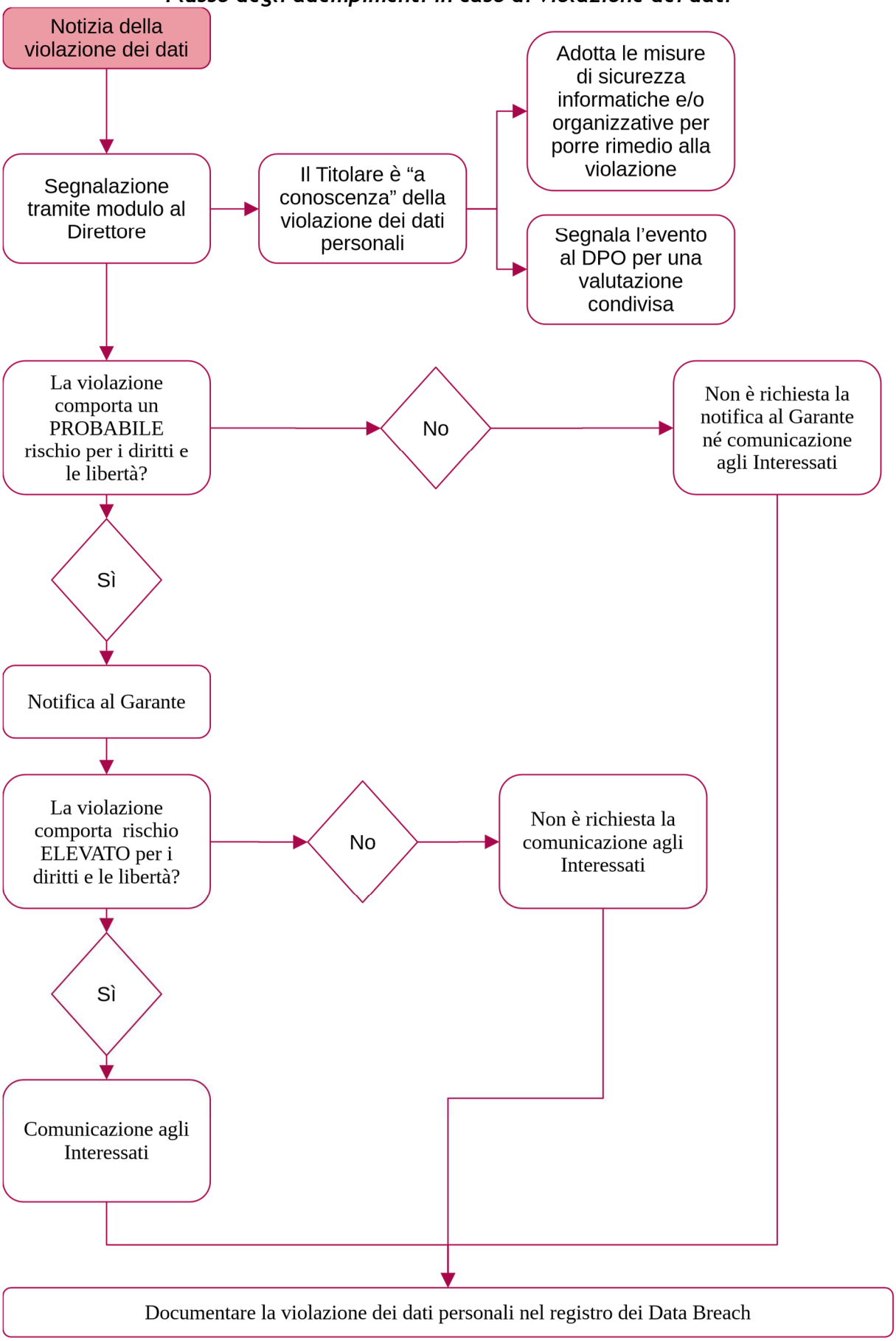
È istituito il "Registro dei Data Breach", come strutturato nell'Allegato E.

Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dall'Autorità di controllo al fine di verificare il rispetto delle disposizioni del GDPR.

Si richiamano espressamente i seguenti documenti:

- Linee guida EDPB 9/2022 in materia di notifica delle violazioni di dati personali (data breach).
- Linee guida EDPB 1/2021 sugli esempi riguardanti la notifica di violazione dei dati.

Flusso degli adempimenti in caso di violazione dei dati



Articolo 34): TRASFERIMENTO DI DATI PERSONALI ALL'ESTERO

Si fa rinvio ai principi dettati dal Regolamento Europeo agli articoli 44 e seguenti, nonché alle indicazioni che fossero dettate, in materia, dal Legislatore nazionale e dal Garante per la protezione dei dati personali.

PARTE TERZA: DIRITTI DELL'INTERESSATO

Articolo 35): DIRITTO DI ACCESSO DELL'INTERESSATO

Come stabilito dall'art. 15 del Regolamento Europeo n. 2016/679, l'Interessato ha il diritto di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) le finalità del trattamento;
b) le categorie di dati personali in questione;
c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
e) l'esistenza del diritto dell'Interessato di chiedere al Titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
f) il diritto di proporre reclamo a un'autorità di controllo;
g) qualora i dati non siano raccolti presso l'Interessato, tutte le informazioni disponibili sulla loro origine;
h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'art. 22 del Regolamento Europeo, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'Interessato.

Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'Interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'art. 46 del Regolamento Europeo relative al trasferimento.

Il Titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'Interessato, il Titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'Interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'Interessato, le informazioni sono fornite in un formato elettronico di uso comune.

Il diritto di ottenere una copia non deve ledere i diritti e le libertà altrui.

Per quanto riguarda, inoltre, le modalità concrete per mezzo delle quali trova attuazione, nell'attuale contesto normativo ed organizzativo, il diritto di accesso, si fa rinvio alle vigenti diposizioni normative e regolamentari emanate, negli anni, dal Legislatore statale nonché dal Garante per la privacy, con particolare riferimento all'ambito sanitario.

Si fa espresso rinvio, in particolare, alle vigenti disposizioni normative in materia di "accesso documentale", di "accesso civico" e di "accesso generalizzato".

Articolo 36): DIRITTO DI RETTIFICA

Come stabilito dall'art. 16 del Regolamento Europeo n. 2016/679, l'Interessato ha il diritto di ottenere dal Titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'Interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Articolo 37): DIRITTO ALLA CANCELLAZIONE (DIRITTO ALL'OBLIO)

Come stabilito dall'art. 17 del Regolamento Europeo n. 2016/679, in capo all'Interessato è riconosciuto il diritto "all'oblio", che si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata.

Si prevede, infatti, l'obbligo per i titolari di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione" (si veda art. 17, paragrafo 2 del Regolamento Europeo).

Articolo 38): DIRITTO DI LIMITAZIONE AL TRATTAMENTO

È esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì anche se l'Interessato chiede la rettifica dei dati (in attesa di tale rettifica da parte del Titolare) o si oppone al loro trattamento ai sensi dell'art. 21 del Regolamento Europeo (in attesa della valutazione da parte del Titolare).

Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la limitazione è vietato a meno che ricorrano determinate circostanze (consenso dell'Interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra persona fisica o giuridica, interesse pubblico rilevante).

Articolo 39): DIRITTO ALLA PORTABILITÀ DEI DATI

Si applica ai trattamenti automatizzati (quindi non si applica agli archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio; in particolare, sono portabili solo i dati trattati con il consenso dell'Interessato o sulla base di un contratto stipulato con l'Interessato (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del Titolare, per esempio), e solo i dati che siano stati "forniti" dall'Interessato al Titolare (si veda il considerando 68 del Regolamento UE).

Inoltre, il Titolare deve essere in grado di trasferire direttamente i dati portabili a un altro Titolare indicato dall'Interessato, se tecnicamente possibile.

Articolo 40): DIRITTO DI OPPOSIZIONE

Come stabilito dall'art. 21 del Regolamento Europeo n. 2016/679, l'Interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'Articolo 6, paragrafo 1, lettere e) o f) del medesimo Regolamento, compresa la profilazione sulla base di tali disposizioni.

Il Titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'Interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Articolo 41): PROCESSO DECISIONALE AUTOMATIZZATO (PROFILAZIONE)

Come stabilito dall'Articolo n. 22 del Regolamento Europeo n. 2016/679, l'Interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

Tale principio non si applica nel caso in cui la decisione:

- sia necessaria per la conclusione o l'esecuzione di un contratto tra l'Interessato e un Titolare del trattamento;
- sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà dei legittimi interessi dell'Interessato;
- si basi sul consenso esplicito dell'Interessato.

Articolo 42): DIRITTI RIGUARDANTI LE PERSONE DECEDUTE

L’art. 2-terdecies del D.lgs. 101/2018 prevede che i diritti di cui agli articoli da 15 a 22 del Regolamento UE riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'Interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione.

L'esercizio di tali diritti non è ammesso nei casi previsti dalla legge o quando, limitatamente all'offerta diretta di servizi della società dell'informazione, l'Interessato lo ha espressamente vietato con dichiarazione scritta presentata al Titolare del trattamento o a quest'ultimo comunicata.

La volontà dell'Interessato di vietare l'esercizio dei diritti deve inoltre risultare in modo non equivoco e deve essere specifica, libera e informata.

In ogni caso, il divieto non può produrre effetti pregiudizievoli per l'esercizio da parte dei terzi dei diritti patrimoniali che derivano dalla morte dell'Interessato nonché del diritto di difendere in giudizio i propri interessi.

DISCIPLINARE SULLE MISURE DI SICUREZZA DEGLI STRUMENTI INFORMATICI A PROTEZIONE DEI DATI PERSONALI

1. FINALITÀ E AMBITO DI APPLICAZIONE

1.1 SCOPO DEL DISCIPLINARE

Il presente disciplinare ha lo scopo di fornire indicazioni per l'utilizzo sicuro ed appropriato delle risorse informatiche (hardware, software, Internet, posta elettronica) date in uso al personale. Il disciplinare si prefigge lo scopo di una gestione controllata, efficace, efficiente e conforme alla normativa tramite:

- l'informazione/formazione di tutto il personale coinvolto;
- l'applicazione del presente disciplinare;
- il monitoraggio del rispetto delle norme impartite con il seguente documento;
- la valutazione del grado di applicazione del presente disciplinare e l'applicazione di opportuni interventi correttivi.

1.2 CAMPO DI APPLICAZIONE

Le disposizioni contenute nel presente documento devono essere adottate e rigorosamente osservate all'interno dell'Ente da tutto il personale dipendente e dai soggetti che nelle varie forme collaborano e prestano la loro opera utilizzando uffici e strumentazione dell'ente, al fine di evitare infrazioni alle norme vigenti.

Gli strumenti informatici oggetto del presente disciplinare sono in uso nell'Ente (in proprietà, noleggio, service, comodato o qualsiasi altra forma contrattuale) e sono messi a disposizione dei Dipendenti/Utenti al fine di permettere il quotidiano svolgimento delle proprie prestazioni lavorative. Essi sono essenzialmente individuabili quali:

- server, computer, fissi o mobili, tablet e altri apparati mobili, sistemi di identificazione e di autenticazione informatica, smartphone concessi in uso;
- Internet, intranet e altri strumenti di scambio di comunicazioni e file, compresi quelli delocalizzati con tecnologia cloud; apparecchiature informatiche necessarie per l'uso di Internet o intranet;
- posta elettronica;
- qualsiasi altro programma e apparecchiatura informatica destinata a memorizzare o a trasmettere dati e informazioni.

Sono esentati dall'applicazione del presente disciplinare, e limitatamente a quanto necessario per il corretto svolgimento delle proprie funzioni, gli Amministratori di Sistema formalmente nominati.

2. ORGANIZZAZIONE E RESPONSABILITÀ

2.1 FORMAZIONE CONTINUA E AGGIORNAMENTI

L'Ente si impegna a garantire che tutto il personale riceva una formazione continua in materia di sicurezza informatica. A tal fine, saranno organizzati corsi periodici che tratteranno tematiche quali la gestione dei dati, le normative sulla protezione dei dati personali, le tecniche di riconoscimento delle minacce informatiche e le migliori pratiche per la protezione dei dati. La partecipazione a tali corsi sarà obbligatoria per tutti i dipendenti e collaboratori, al fine di mantenere alta la consapevolezza e la preparazione del personale rispetto alle attuali minacce informatiche.

2.2 SERVIZIO DI ASSISTENZA A MANUTENZIONE

L'Ente rende noto che l'attuale ditta esterna affidataria del servizio di assistenza e manutenzione della rete informatica, nella qualità di Responsabile esterno del trattamento e nella fattispecie in qualità di Amministratore di Sistema, è autorizzata a compiere interventi nel sistema informatico, diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi.

Detti interventi potranno anche comportare in qualunque momento, e anche in assenza dell'affidatario, l'accesso agli strumenti hardware e di conseguenza anche ai dati trattati da ciascuno, ivi compresi gli archivi su Pc e Server.

La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Ente si applica anche in caso di assenza prolungata od impedimento del dipendente.

La ditta esterna di cui sopra ha inoltre la facoltà di collegarsi, previa autorizzazione dell'Utente, mediante visualizzazione di un indicatore visivo sul monitor che segnala la connessione in remoto del tecnico informatico, e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus informatici in genere. L'intervento di norma viene effettuato esclusivamente su chiamata dell'Utente ma, in caso di oggettiva necessità, ad esempio a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico la cui risoluzione richieda l'accesso ai sistemi affidati al dipendente assente, l'intervento sarà comunque erogato, utilizzando le credenziali di Amministratore di sistema. In quest'ultimo caso, e sempre fatta salva la necessaria tempestività ed efficacia dell'intervento, verrà data formale comunicazione via e-mail della necessità dell'intervento stesso o dell'avvenuto intervento.

3. GESTIONE DELLE CREDENZIALI E ACCESSI

3.1 CREDENZIALI DI AUTENTICAZIONE

Ad ogni Utente "incaricato" sono assegnate o associate individualmente una o più credenziali per l'autenticazione (identificativo e password) necessarie per accedere alle risorse informatiche e alle applicazioni software; l'incaricato deve adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo. Al fine di agevolare l'Utente nella corretta gestione delle proprie password, possono essere utilizzati software di password manager.

Le credenziali di autenticazione per l'accesso alla rete aziendale vengono inizialmente assegnate dall'Amministratore di Sistema o dal Responsabile del Servizio ICT e successivamente obbligatoriamente reimpostate dal dipendente stesso secondo le modalità operative di seguito meglio specificate.

La credenziale di autenticazione (login) consiste in un codice per l'identificazione dell'Utente (user id), assegnato ed associato ad una parola chiave (password) riservata e modificata dall'Utente al primo accesso. Essa dovrà essere memorizzata, custodita con la massima diligenza e non divulgata.

3.2 REQUISITI PER LE PASSWORD

La password deve:

- essere composta da almeno 12 caratteri per utente standard;
- non contenere riferimenti all'Utente (es. nome o cognome);
- non essere composte da semplici sequenze di tasti (es. "qwerty"), o da ripetizioni del proprio nome utente (es. "rossirossi");
- non essere utilizzata per accessi a sistemi diversi (es. accesso al sistema operativo, software gestionale, posta elettronica, portali web).

Laddove possibile, è consigliato utilizzare sistemi di accesso multi-fattore.

La password di accesso di ciascun Utente dovrà essere reimpostata a cura dell'Utente periodicamente, almeno una volta all'anno. Nel caso non fosse possibile inserire tale procedura in automatico sarà cura dell'Utente inserire una nuova password, diversa dalla precedente.

Intervalli di tempo più ravvicinati, secondo i maggiori esperti di sicurezza informatica, produrrebbero effetti negativi incentivando l'Utente ad usare solo banali cambi di password tra la precedente e la nuova, al fine di poterla facilmente ricordare.

Nel caso in cui l'Utente venga a conoscenza del fatto che la password sia stata violata deve procedere senza ritardo ad informare il proprio Responsabile del servizio e l'assistenza tecnica, nonché a sostituire la password ovunque sia stata impostata.

4. UTILIZZO DEI DISPOSITIVI INFORMATICI

4.1 PERSONAL COMPUTER (Fissi e Portatili)

Per l'utilizzo dei personal computer, sia fissi che portatili, oltre a tablet e altri device similari, l'Utente deve seguire le seguenti indicazioni:

- il computer deve essere spento ogni giorno prima di lasciare gli uffici nonché in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo;
- l'Utente deve impostare il blocco schermo automatico che si attivi in caso di inutilizzo della risorsa per un periodo superiore ai 5 minuti;
- non è consentito lasciare un elaboratore incustodito acceso o non bloccato; ciò infatti potrebbe permettere l'utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. Di conseguenza, qualora ci si allontani dalla propria postazione, occorre bloccare il computer (attivare la schermata di protezione) o disconnettersi;
- i dati devono essere salvati esclusivamente sul server, e non in locale, in modo da poter essere oggetto di backup;
- si possono installare i soli software, e utilizzare i soli servizi web, presenti nella White List dell'Appendice "Liste software e servizi"; in ogni caso i software ed i servizi dovranno essere relativi all'attività lavorativa e provenienti da siti noti e sicuri, previo accertamento inoltre che ciò sia conforme alla licenza d'uso;
- eventuali altri software/servizi web che si rendessero necessari possono essere installati/utilizzati solamente previa autorizzazione del Responsabile di Servizio ICT;
- non è consentito collegare alla rete informatica personal computer o pc portatili e, più in generale, qualsiasi dispositivo hardware non ascrivibili alla proprietà o altra forma di possesso dell'Ente, salvo specifica autorizzazione del Responsabile del Servizio ICT.

4.2 DISPOSITIVI ELETRONICI PORTATILI

L'Utente è responsabile dell'integrità dei dispositivi elettronici portatili (computer portatile, tablet, smartphone, …) affidatogli dall'Ente e dei dati ivi contenuti.

L'Utente è tenuto a custodirlo con diligenza sia durante l'utilizzo nel luogo di lavoro sia durante i suoi spostamenti. A tali dispositivi si applicano le regole di utilizzo previste per i personal computer.

Nel caso di utilizzo condiviso con altri Dipendenti/Utenti, prima della riconsegna occorre provvedere:

- alla rimozione definitiva di eventuali file elaborati contenenti dati personali;
- alla disconnessione dal servizio/software utilizzato.

È inoltre vietato il salvataggio delle password nel browser.

I dispositivi portatili contenenti dati personali dovranno essere criptati, al fine di evitare, in caso di furto o di smarrimento, l'accesso ai dati stessi da parte di soggetti non autorizzati. Tale operazione deve essere eseguita dal Responsabile del Servizio ICT o dall'assistenza tecnica.

All'atto della cessazione/interruzione del rapporto di lavoro o dell'attività lavorativa svolta a qualsiasi titolo, ferma restando la disabilitazione all'uso degli applicativi e delle funzionalità da parte del Servizio ICT, è fatto obbligo di restituzione delle strumentazioni elettroniche (pc portatili, tablet, cellulari, kit di firma elettronica ecc.) già affidate per l'esplicazione delle funzioni connesse al rapporto di lavoro.

4.3 SUPPORTI DI MEMORIZZAZIONE RIMOVIBILI (Hard disk, Pen drive USB, …)

L'utilizzo di supporti di memorizzazione rimovibili è normalmente vietato.

In caso di necessità può essere chiesta una autorizzazione in deroga al Responsabile del Servizio ICT per l'utilizzo di supporti di proprietà dell'Ente opportunatamente controllati.

I supporti di memorizzazione, se contenenti dati personali, dovranno essere criptati, al fine di evitare, in caso di furto o di smarrimento, l'accesso ai dati stessi da parte di soggetti non autorizzati. Tale operazione deve essere eseguita dal Responsabile del Servizio ICT o dall'assistenza tecnica.

È vietato consegnare a terzi supporti già utilizzati per la memorizzazione di informazioni o di dati personali, anche se cancellati, in quanto è tecnicamente possibile il loro recupero anche dopo l'intervenuta cancellazione.

L'Utente è tenuto a informare immediatamente il proprio responsabile, il Servizio ICT e il Responsabile della Protezione dei Dati, anche ai sensi della procedura di gestione delle violazioni di dati personali, di qualsiasi danno, furto o perdita di apparati, software e/o dati in proprio possesso, fatti salvi gli obblighi di denuncia alle autorità competenti.

4.4 POLITICA DI UTILIZZO DEI DISPOSITIVI PERSONALI (BYOD)

L'Ente riconosce l'importanza e la praticità dell'utilizzo di dispositivi personali (Bring Your Own Device - BYOD) per scopi lavorativi. Tuttavia, per garantire la sicurezza dei dati aziendali e la protezione delle informazioni sensibili, è necessario seguire le seguenti linee guida:

Autorizzazione e Registrazione: prima di utilizzare un dispositivo personale per attività lavorative, l'Utente deve richiedere e ottenere l'autorizzazione dal Responsabile del Servizio ICT.

Misure di Sicurezza: i Dipendenti/Utenti sono tenuti a garantire che i dispositivi personali siano protetti da misure di sicurezza adeguate, tra cui:

- installazione di software antivirus aggiornato;
- attivazione di un sistema di blocco dello schermo tramite password o biometria;
- aggiornamento regolare del sistema operativo e delle applicazioni per garantire la protezione contro vulnerabilità note.

In caso di utilizzo condiviso del dispositivo con altri familiari è necessario creare un profilo separato nel sistema operativo per lo svolgimento dell'attività lavorativa, con credenziali conosciute al solo lavoratore.

Accesso ai Dati Aziendali: l'accesso ai dati aziendali deve avvenire esclusivamente tramite applicazioni e reti autorizzate dall'Ente. È vietato memorizzare dati aziendali su dispositivi personali senza l'approvazione del Responsabile di servizio. Qualora sia necessario, i dati devono essere archiviati in modo sicuro, ad esempio utilizzando soluzioni di cloud aziendale approvate.

Segnalazione di smarrimento o furto: in caso di smarrimento o furto del dispositivo personale, l'Utente deve informare immediatamente il proprio Responsabile di servizio e il Responsabile del Servizio ICT.

Disattivazione e Rimozione dei Dati: al termine del rapporto di lavoro l'Utente è tenuto a disattivare l'accesso ai dati aziendali e a rimuovere qualsiasi informazione lavorativa dal dispositivo personale. È responsabilità dell'Utente garantire che i dati aziendali non siano più accessibili dopo la cessazione del rapporto di lavoro.

Monitoraggio e Audit: l'Ente si riserva il diritto di monitorare l'uso dei dispositivi personali per garantire la conformità a questa politica. I Dipendenti/Utenti devono essere consapevoli che l'uso di dispositivi personali per scopi lavorativi può essere soggetto a audit e verifiche da parte del personale autorizzato.

È vietato, se non per casi eccezionali di urgenza e di indisponibilità di dispositivi aziendali, l'utilizzo di dispositivi di proprietà del dipendente, compresi smartphone e relativi servizi, per contattare fornitori, ospiti e persone di riferimento degli ospiti, o altre tipologie di utenti.

4.5 STAMPANTI E FOTOCOPIATORI

Qualora l'Utente dovesse stampare documenti contenenti dati o informazioni riservate, dovrà aver cura di monitorare la stampante e preservare, limitatamente alle oggettive possibilità, la conoscibilità di tali dati o informazioni da parte di terzi non autorizzati.

Nel caso di stampa di dati particolari o giudiziari, ai sensi degli artt. 9 e 10 del Regolamento UE 679/2016, è necessario abilitare la funzione di "stampa in attesa / sospensione", qualora disponibile, in modo che la stampa sia avviata solo con l'intervento in presenza dell'incaricato/autorizzato al trattamento dei dati. Le istruzioni per il corretto utilizzo sono riportate nell'Appendice "Stampa in attesa".

È fatto divieto di lasciare documenti incustoditi nei fotocopiatori e nelle stampanti condivise.

5. COMUNICAZIONI ELETTRONICHE

5.1 UTILIZZO DELLA POSTA ELETTRONICA

Il servizio di posta elettronica è un mezzo istituzionale di comunicazione aziendale e il suo utilizzo deve avvenire nel rispetto delle norme in materia di protezione dei dati personali.

La prudenza nella gestione delle e-mail ricevute contribuisce in grande misura alla sicurezza dei dati presenti nei sistemi informativi. Il rispetto delle semplici regole che seguono si rendono quindi necessarie per una adeguata protezione contro gran parte delle attuali minacce:

- diffidare delle e-mail di cui non si conosce l'indirizzo del mittente; in questo caso non aprire mai gli allegati o i programmi ivi contenuti, né selezionare i link indicati;
- anche se il messaggio e-mail sembra provenire da un mittente conosciuto, prestare attenzione al suo contenuto e alla sua "attendibilità", in quanto risulta molto semplice inviare messaggi e-mail a nome di altri; in caso di dubbio contattare (anche telefonicamente) il mittente per verificare l'autenticità del messaggio;
- aprire unicamente i file o i programmi provenienti da fonti affidabili e solo previa verifica con un programma antivirus aggiornato;
- non aprire mai gli allegati ad e-mail provvisti di due estensioni (es. picture.bmp, .exe, .vbs) e non lasciarsi ingannare dall'icona di simili file;

- non rispondere agli spam: rispondere ad un messaggio di spam equivale ad informare lo spammer che l'indirizzo e-mail è valido e quindi questi invierà ulteriori spam oppure metterà il vostro indirizzo a disposizione di altri spammer; particolare attenzione va portata agli spam con l'opzione di "cancellazione dall'elenco" in cui si promette la cancellazione dall'elenco di distribuzione tramite l'invio di una e-mail con un determinato contenuto;
- avvertimenti di pericolo di virus inviati tramite e-mail: nella maggior parte dei casi sono false informazioni; non eseguire mai, in nessun caso, le raccomandazioni ivi contenute; questo con particolare riferimento a cancellazione di file, installazione di un determinato programma, inoltro dell'informazione ai conoscenti;
- in caso di dubbi contattare sempre il Responsabile del Servizio ICT.

Le caselle e-mail aziendali, con struttura del tipo ufficio/nucleo/sede@dominio.it (per es. info@casanostravaldastico.it), si devono intendere come accessibili a più dipendenti dell'ufficio/nucleo/sede, pertanto non può essere garantita la riservatezza delle comunicazioni personali.

Anche eventuali "alias" nominativi collegati a caselle "aziendali" seguono la medesima regola.

Quando si inviano e-mail a più destinatari esterni, come familiari o dipendenti, è necessario utilizzare il campo Ccn (o Bcc in inglese). Questo accorgimento consente di nascondere gli indirizzi e-mail degli altri destinatari, garantendo così la riservatezza dei dati personali. È importante ricordare che, oltre agli indirizzi e-mail, potrebbero essere condivisi anche informazioni sensibili, come dati relativi allo stato di salute, ad esempio in comunicazioni destinate a ospiti con specifiche patologie.

In caso di assenza prolungata programmata dell'Utente, si raccomanda allo stesso di attivare il sistema di risposta automatica ai messaggi di posta elettronica ricevuti indicando, nel messaggio di accompagnamento, le coordinate di un collega che può essere contattato in sua assenza e/o altre modalità utili di contatto della Struttura organizzativa presso cui presta la propria attività lavorativa.

Alla cessazione del rapporto di lavoro, le eventuali caselle e-mail nominative (ad es. nome.cognome@dominio.it) devono essere immediatamente disattivate dal Responsabile del Servizio ICT, con impostazione di un messaggio automatico di risposta di avviso al mittente.

5.2 NAVIGAZIONE INTERNET

Gran parte dei pericoli per la sicurezza del sistema informativo vengono corsi durante la navigazione in Internet. Molti di questi pericoli possono essere evitati adottando opportune misure comportamentali, pertanto i Dipendenti/Utenti devono osservare le seguenti indicazioni:

- effettuare l'accesso solamente a siti web sicuri e noti;
- non scaricare mai programmi sconosciuti da Internet prima di averne accertato la provenienza.
- non comunicare mai a nessuno le proprie credenziali di accesso (nome di utente e password), nessun fornitore di servizi serio chiederà la vostra password (nemmeno telefonicamente), anche quando la richiesta appare credibile;
- utilizzare sempre l'apposita notifica di chiusura ("logout") quando si esce da un'applicazione web che abbia richiesto l'introduzione delle proprie credenziali di accesso;
- evitate di rivelare dati personali durante la compilazione di moduli web.

6. PROTEZIONE DA MINACCE INFORMATICHE

6.1 PROTEZIONE DA VIRUS

Le postazioni di lavoro sono protette da software antivirus aggiornato quotidianamente.

Ogni Utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico. Questa fattispecie può accadere mediante virus o malware, proveniente da dati e/o software

importati/installati dall'Utente, che si auto-installano, all'insaputa dell'Utente, all'interno del Pc, infettandolo e diffondendosi nella rete informatica aziendale.

Nel caso in cui il software antivirus rilevi e non disinfetti la presenza di un virus, l'Utente dovrà immediatamente sospendere ogni elaborazione in corso e segnalare l'accaduto al Responsabile del Servizio ICT.

Ogni dispositivo di memorizzazione esterna dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e nel caso venga rilevato un virus, dovrà essere prontamente consegnato all'assistenza tecnica che provvederà ad effettuare le dovute operazioni di disinfezione.

6.2 PROCEDURE DI RISPOSTA AGLI INCIDENTI

L'Ente ha predisposto un protocollo di gestione degli incidenti di sicurezza informatica al fine di garantire una risposta efficace e tempestiva a qualsiasi violazione dei dati o attacco informatico. Le seguenti procedure devono essere seguite da tutti i Dipendenti/Utenti in caso di sospetta o confermata compromissione della sicurezza:

Identificazione dell'Incidente: i Dipendenti/Utenti devono essere in grado di riconoscere i segnali di un possibile incidente di sicurezza, che possono includere:

- accessi non autorizzati ai sistemi o ai dati;
- comportamenti anomali dei dispositivi o delle applicazioni;
- ricezione di comunicazioni sospette, come e-mail di phishing o avvisi di sicurezza falsi.

Segnalazione immediata: in caso di sospetto o conferma di un incidente, l'Utente deve informare immediatamente il Responsabile del Servizio ICT. La segnalazione deve avvenire senza indugi, fornendo dettagli chiari e completi sull'incidente, inclusi:

- data e ora dell'evento.
- descrizione dell'incidente e delle circostanze.
- eventuali azioni già intraprese dall'Utente.

Contenimento della minaccia: una volta segnalato l'incidente, il Responsabile del Servizio ICT e il team di assistenza tecnica valuteranno la situazione e adotteranno misure per contenere l'incidente. Ciò può includere:

- disconnessione del dispositivo compromesso dalla rete;
- blocco temporaneo degli accessi agli account interessati;
- isolamento dei dati o dei sistemi coinvolti.

Analisi e Valutazione: dopo il contenimento, sarà condotta un'analisi approfondita dell'incidente per determinarne la causa e l'impatto. Questa fase può includere:

- raccolta di prove digitali;
- analisi dei log di accesso e delle attività di sistema;
- interviste con i Dipendenti/Utenti coinvolti.

Risoluzione e ripristino: una volta completata l'analisi, il team di assistenza tecnica procederà alla risoluzione dell'incidente. Le azioni possono includere:

- rimozione di malware o virus dai sistemi;
- ripristino dei dati da backup sicuri;
- ripristino delle configurazioni di sicurezza.

Comunicazione: è fondamentale mantenere una comunicazione chiara, tempestiva e tracciata durante tutto il processo di gestione dell'incidente. I Dipendenti/Utenti coinvolti e le parti interessate devono essere informati sui progressi e sulle azioni intraprese. In caso di violazioni significative, potrebbe essere necessario informare anche le autorità competenti e gli utenti interessati, in conformità con le normative vigenti.

Documentazione: tutti gli incidenti devono essere documentati in modo dettagliato, inclusi i passaggi seguiti per la gestione dell'incidente, le decisioni prese e le lezioni apprese. Questa documentazione sarà utilizzata per migliorare le procedure di risposta agli incidenti e per la formazione futura del personale.

Revisione e miglioramento: dopo la risoluzione dell'incidente, sarà condotta una revisione post-incidente per valutare l'efficacia della risposta e identificare aree di miglioramento. Le raccomandazioni emerse dalla revisione saranno integrate nelle politiche e nelle procedure di sicurezza dell'Ente.

7. INTELLIGENZA ARTIFICIALE

Nella pubblica amministrazione si stanno diffondendo strumenti di IA che possono essere suddivisi in due grandi categorie:

1. strumenti disponibili pubblicamente online;
2. soluzioni fornite da aziende specializzate.

Ognuna di queste tipologie ha caratteristiche, vantaggi e limiti da considerare attentamente.

7.1 RISCHI PRINCIPALI

L'impiego dell'IA può generare problematiche di varia natura. I rischi più comuni comprendono:

- Condivisione involontaria di dati personali o sensibili: l'inserimento di dati identificativi in strumenti IA online potrebbe violare il GDPR e compromettere la riservatezza.
- Bias (distorsioni o pregiudizi nei dati o negli algoritmi): gli algoritmi possono riflettere discriminazioni o errori presenti nei dati di addestramento.
- Affidabilità non garantita (risposte sbagliate): le IA possono generare informazioni scorrette o completamente inventate.
- Assenza di tracciabilità e responsabilità in assenza di supervisione umana: l'automazione non deve mai sostituire il controllo umano, necessario per ogni decisione amministrativa.

Tutti questi rischi devono essere valutati prima dell'adozione di qualsiasi soluzione IA, privilegiando trasparenza, verifica dei risultati e corretto trattamento dei dati.

7.2 STRUMENTI ONLINE PUBBLICI

Si tratta di strumenti ampiamente disponibili sul web, spesso utilizzabili gratuitamente o tramite abbonamento, che forniscono supporto generico nella generazione di testi, immagini, risposte e sintesi. Sono i più diffusi e utilizzati anche al di fuori dell'ambiente pubblico, ma richiedono attenzione nell'uso dei dati inseriti. Esempi:

- Duck.ai: possibilità di utilizzare vari modelli di IA, limitando la condivisione di dati personali
- HuggingChat: possibilità di utilizzare vari modelli di IA
- ChatGPT (OpenAI): generazione testi, sintesi, risposte a domande
- Perplexity, Claude: assistenti virtuali avanzati
- DALL·E, Midjourney: creazione immagini artificiali

Utilizzo consentito:
È possibile utilizzare tali strumenti per elaborazioni prive di dati personali. Nel caso in cui i documenti contengano dati personali, prima dell'inserimento nei modelli di IA risulta necessario provvedere alla anonimizzazione, o alla pseudonimizzazione, dei dati.

Il risultato prodotto andrà sempre revisionato da persona umana prima di qualsiasi utilizzo.

7.3 SOLUZIONI FORNITE DA AZIENDE SPECIALIZZATE

Sono soluzioni verticali fornite da aziende specializzate, pensate per specifiche esigenze della PA. Vengono usate, ad esempio, per analisi di rischio, trasparenza amministrativa, monitoraggio e gestione di grandi volumi di dati. Possono prevedere contratti di fornitura, audit e valutazioni di impatto. Strumenti verticali utilizzati per:

- gestione documentale automatica
- analisi predittive
- anticorruzione e trasparenza
- supporto alle gare e contratti pubblici

Alla data di approvazione del presente disciplinare l'Ente non ha adottato alcuna di queste soluzioni di IA.

Utilizzo consentito:
È possibile utilizzare tali strumenti seguendo i principi e le indicazioni del Regolamento (UE) 2024/1689 "Regolamento sull'Intelligenza Artificiale – AI Act" e delle "Linee Guida per l'adozione dell'IA nella PA" prodotte da Agid (ad oggi in fase di consultazione pubblica).

8. GESTIONE DEL CICLO DI VITA

8.1 CESSAZIONE DEI RAPPORTI DI LAVORO

Al termine del rapporto di lavoro, il Servizio ICT provvede a:

- disabilitare l'accesso agli applicativi e alle funzionalità;
- verificare la restituzione delle strumentazioni elettroniche;
- disattivare l'eventuale casella e-mail nominativa, abilitando una risposta automatica che informi il mittente che la casella non è più attiva e una indicazione di indirizzo e-mail alternativo.

8.2 SMALTIMENTO DEI DISPOSITIVI ELETTRONICI

In caso di smaltimento di dispositivi elettronici contenenti dati personali, l'Utente deve accertarsi che siano fisicamente distrutti ovvero cancellati tramite opportuni software di formattazione approfondita. In ogni caso si rende opportuno consultare il Responsabile del Servizio ICT.

APPENDICE: “LISTE SOFTWARE E SERVIZI”

WHITELIST (Software e Servizi Internet Autorizzati)

Questa sezione elenca i software e i servizi internet che sono stati approvati per l'uso all'interno dell'Ente. I Dipendenti/Utenti sono tenuti a utilizzare esclusivamente i software e i servizi presenti in questa lista per garantire la sicurezza dei dati e la conformità alle normative.

Software Autorizzati – Personal Computer 

Sistemi operativi

- Ms Windows 10
- Ms Windows 11
- Linux (varie distribuzioni)

Gestionali:

- Ambiente Halley (gestionale area amministrativa)
- Zucchetti Healthcare Cartella Socio Sanitaria, Contabilità Utenti (gestionale area socio-sanitaria e manutentiva)
- Zucchetti Healthcare Servizi di Manutenzione, Richieste da reparto (gestionale servizi manutentivi)

Suite per ufficio:

- Libreoffice
- Onlyoffice
- Notepad++
- Ms Office (in locale)

Posta elettronica

- Thunderbird
- Ms Outlook *(sconsigliato)*

Browser web:

- Mozilla Firefox
- Brave
- Librewolf
- Edge *(sconsigliato)*
- Chrome *(sconsigliato)*

Software di grafica e design:

- GIMP
- Ms Paint
- Irfanview

Gestione PDF

- Okular
- Onlyoffice
- PDF creator
- PDF24 Creator
- PDF x-change viewer
- Acrobat reader

Firma digitale

- Aruba sign
- Namirial sign
- GoSign desktop (ex Dike)

Gestore di password

- Keepass XC
- Keepass

Gestione file compressi

- 7-zip

Desktop remoto

- Software forniti dalle software house per l'assistenza: Boxxapps (per Halley) e Zucchetti utilizzano i propri software
- Anydesk (per altri usi)

Registrazione audio-video

- OBS studio

Player multimediale

- VLC

Software Autorizzati – Smartphone e tablet 

Sistemi operativi

- Android (vers. 10 o superiore)

Gestionali:

- Zucchetti Healthcare CSS 2.0 (gestionale area socio-sanitaria)

Suite per ufficio:

- Collabora Office

Posta elettronica

- Thunderbird
- K9 mail

Messaggistica istantanea

- Signal / Molly

Browser web:

- Mozilla Firefox
- Brave
- Duckduckgo
- Chrome *(sconsigliato)*

Software di grafica e design:

- Image toolbox

Gestione PDF

- *In browser*

Gestore di password

- Keepass DX

Player multimediale

- VLC

Lettura QR code

- QR scanner (Secuso) scaricabile da F-Droid

Galleria fotografica

- Aves Galleria

Servizi Internet Autorizzati:

Tutti i portali istituzionali (INPS, InPA, PerlaPA, INAIL, …)

Gestionali

- Portale per la gestione del personale HRMS (https://hrms.accatre-stp.it/sp/istcavpaolosartori)
- Servizi di Accatre (https://www.x-desk.it/istitutopaolosartori)
- Servizi Cloud dell'Ente (https://cloud.casanostravaldastico.it), che comprende servizi come condivisione file, videoconferenza, posta elettronica, contatti, calendario, note, sondaggi, moduli, task

Posta elettronica

- Webmail istituzionale (Zimbra - https://mail-casanostravaldastico.telemar.it)

Motori di ricerca

- DuckduckGo (https://duckduckgo.com)
- SearXNG (https://searx.stream – o altre istanze UE)

Gestore di password

- Bitwarden (su server UE - https://bitwarden.com)

Gestione PDF

- PDF24 (https://www.pdf24.org/it) – per documenti privi di dati personali
- Stirling PDF (https://pdf.serviziliberi.it) – per documenti privi di dati personali

Videoconferenza

- Nextcloud Talk (https://cloud.casanostravaldastico.it)
- Jitsi Meet su istanza fornita dal GARR (https://open.meet.garr.it)
- Kmeet (https://www.infomaniak.com/it/ksuite/kmeet)

Traduttori

- Deepl (https://www.deepl.com/it/translator)
- Libre Translate (https://traduzioni.serviziliberi.it/)

Condivisione file

- Nextcloud File (https://cloud.casanostravaldastico.it)
- SwissTransfer (https://www.swisstransfer.com/it-it)
- Send (https://send.vis.ee)

Forms e sondaggi

- Nextcloud Sondaggi e Moduli (https://cloud.casanostravaldastico.it)

Accorciatori di URL

- Savmrl (https://www.savmrl.it)

BLACKLIST (Software e Servizi Internet Vietati)

Questa sezione elenca i software e i servizi internet che non possono essere utilizzati all'interno dell'Ente. L'uso di questi strumenti è vietato per motivi di sicurezza e protezione dei dati.

Software Vietati:

- Qualsiasi software non presente nella sezione "whitelist"
- Whatsapp

Servizi Internet Vietati:

- Qualsiasi servizio utilizzando account personali e non aziendali
- Google Calendar, Gmail, Documenti

DEROGHE (Software e Servizi Utilizzabili in Deroga)

Questa sezione consente l'uso di software e servizi non presenti nella whitelist, previa autorizzazione. I Dipendenti/Utenti devono richiedere una deroga specifica al proprio Responsabile di servizio, fornendo motivazioni valide per l'uso di tali strumenti.

Software Utilizzabili in Deroga:

Nome del software	Motivo della deroga
Whatsapp	Per il solo smartphone in dotazione all'ufficio amministrativo, per contatti veloci con i fornitori. Rimane vietato l'utilizzo con dipendenti, ospiti e loro familiari.

Servizi Internet Utilizzabili in Deroga:

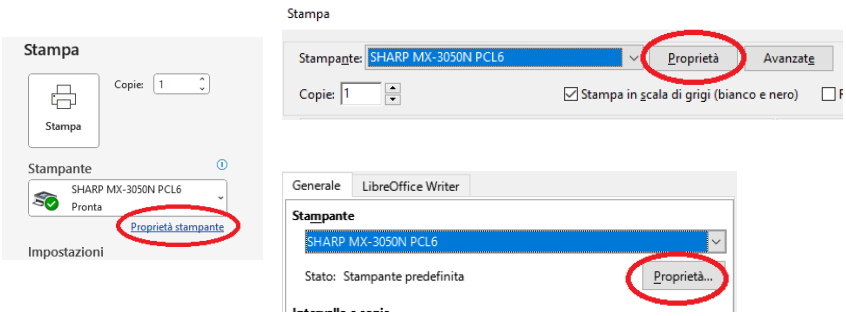
Nome del servizio	URL	Motivo della deroga
Google Meet	https://workspace.google.com/products/meet/	In caso di invito da parte di terze parti, dovuto al largo utilizzo del servizio.
Zoom	https://www.zoom.us	In caso di invito da parte di terze parti, dovuto al largo utilizzo del servizio.
Teams	https://www.microsoft.com/en-us/microsoft-teams/log-in	In caso di invito da parte di terze parti, dovuto al largo utilizzo del servizio.

APPENDICE: “STAMPA IN ATTESA”

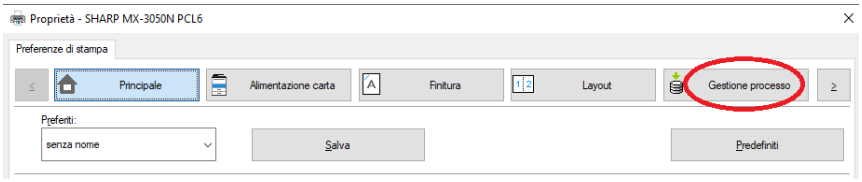
Le stampanti-fotocopiatrici in dotazione all’Ente sono dotate di sistema di protezione e di sospensione della stampa finché non intervenga manualmente l’incaricato/autorizzato al trattamento dei dati.

Per attivare tale funzione, al momento della stampa, occorre andare in:

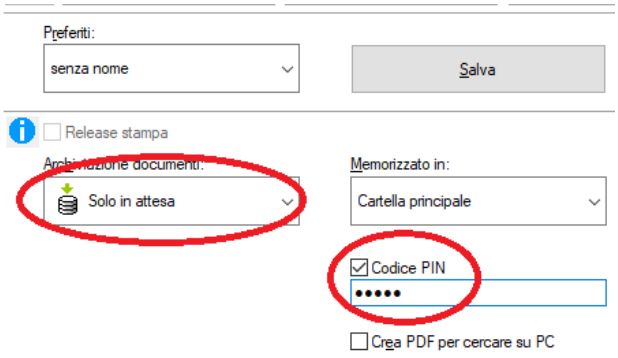
1. “Proprietà stampante” (la schermata può variare in base al software utilizzato):



2. Gestione processo:



3. In Archiviazione documenti, selezionare “Solo in attesa”, poi apporre il flag nel campo “Codice PIN” ed inserire un PIN di sicurezza (minimo 5 caratteri) che dovrà essere digitato per sbloccare la stampa:



4. Sulla stampante, selezionare il tasto “Recupera file disco fisso”:

5. Selezionare “Cartella principale”
6. Selezionare il file da stampare
7. Immettere il PIN inserito in precedenza
8. Spuntare il flag “Stampa ed elimina dati”
9. Selezionare “Stampa adesso”

Registro delle attività di trattamento
(art. 30 Reg. EU 679/2016)

Titolare del trattamento

Comune di Valdastico – Istituzione “Cav. Paolo Sartori”

Forma giuridica	Istituzione comunale ai sensi dell’art. 114 del D.Lgs. 267/2000. La personalità giuridica è in capo al Comune di Valdastico.
Indirizzo della sede	Via Cav. Paolo Sartori n. 20 – 36040 Valdastico (VI)
Dati di contatto del Titolare	Telefono: 0445-745029 i. 3 E-mail: info@casanostravaldastico.it PEC: casanostravaldastico@pecveneto.it
Codice fiscale e Partita IVA	C.F. 84001010242 – P. IVA 01513240240

Responsabile della protezione dei dati (RPD-DPO)

In4data di Finco Matteo – soggetto designato Finco Eric

Dati di contatto del RPD-DPO	E-mail: info@in4data.it PEC: legal@pec.in4data.it
Partita IVA	P. IVA 04477810248

Rappresentante

Non presente

Trattamenti effettuati in qualità di TITOLARE del trattamento

Registro dei trattamenti

Unità Organizzativa	Denominazione del trattamento (se individuata)	Finalità del trattamento *	Articolo 6 (base giuridica su cui si fonda il trattamento)	Articolo 9 (base giuridica per il trattamento di particolari categorie di dati)	Articolo 10 (base giuridica per il trattamento di particolari categorie di dati)	Software, Database, Manutenzione	Denominazione e dati di contatto del contitolare (se presente)	Categorie di interessati *	Categorie di dati personali *	Categorie di destinatari a cui i dati sono o possono essere comunicati *	Denominazione responsabili esterni (se presenti)	Paesi Terzi o organizzazioni internazionali verso cui i dati possono essere trasferiti *	Indicazione garanzie adottate per il trasferimento internazionale (se applicabile) *	Periodo di conservazione dei dati (se possibile) *	Descrizione generale delle misure di sicurezza adottate (se possibile) *	Valutazione d'impatto sulla protezione dei dati personali (DPIA)		
																Valutazione richiesta?	Fase della Valutazione	Indicazione della Valutazione (DPIA) – estremi
Servizio Gestione delle Risorse Umane	**Concorsi pubblici e selezione del personale**	Espletamento delle attività selettive	Esecuzione di misure precontrattuali (art. 6, comma 1, lett. b, del GDPR) Obbligo legale (art. 6, comma 1, lett. c, del GDPR) Esecuzione di un compito di interesse pubblico (art. 6, comma 1, lett. e, del GDPR)	Assolvere obblighi ed esercitare i diritti specifici del titolare del trattamento in materia di diritto del lavoro (art. 9, comma 2, lett. b, del GDPR) Motivi di interesse pubblico rilevante (art. 9, comma 2, lett. g, del GDPR e art. 2-sexies, comma 2, lett. dd, del D.Lgs. 196/2013) Esercitare un diritto in sede giudiziaria (art. 9, comma 2, lett. f, del GDPR)	Trattamento autorizzato da norme di legge (art. 10 del GDPR e art. 2-octies, comma 3, lett. a, del D.Lgs. 196/2003)	File server in rete, caselle e-mail, portale inPA, sezione Amministrazione trasparente del sito istituzionale	-	Candidati ai concorsi / selezioni	Dati comuni, dati particolari, dati giudiziari	Membri esterni delle commissioni concorso, Medico competente, Portale inPA	Dipartimento della funzione pubblica della Presidenza del Consiglio dei ministri (nomina del 13.01.2025), NEXT.ORG Srls (Amministratore di sistema – nomina del 15.11.2021) Halley Veneto Srl (software gestionale – nomina del 25.11.2022) Accatre Srl (conservazione sostitutiva – nomina del 25.11.2022)	-	-	1 anno dalla scadenza dei termini per i ricorsi per i candidati non in graduatoria, termine di validità della graduatoria per i candidati in graduatoria finale, permanente per i candidati assunti	Protezione degli accessi logici, Designazione degli incaricati al trattamento, Formazione degli incaricati, Protezione degli accessi fisici, Minimizzazione dei dati trattati, Nomina dei RTD, Backup dei dati, Firewall di rete, Software antivirus, Impianto antincendio	-	-	-
Servizio Gestione delle Risorse Umane	**Gestione del personale assunto**	Gestione amministrativa del personale assunto	Esecuzione di misure precontrattuali (art. 6, comma 1, lett. b, del GDPR) Obbligo legale (art. 6, comma 1, lett. c, del GDPR) Esecuzione di un compito di interesse pubblico (art. 6, comma 1, lett. e, del GDPR)	Assolvere obblighi ed esercitare i diritti specifici del titolare del trattamento in materia di diritto del lavoro (art. 9, comma 2, lett. b, del GDPR) Motivi di interesse pubblico rilevante (art. 9, comma 2, lett. g, del GDPR e art. 2-sexies, comma 2, lett. dd, del D.Lgs. 196/2013) Esercitare un diritto in sede giudiziaria (art. 9, comma 2, lett. f, del GDPR)	Trattamento autorizzato da norme di legge (art. 10 del GDPR e art. 2-octies, comma 3, lett. a, del D.Lgs. 196/2003)	File server in rete, caselle e-mail Halley, portale HRMS, cartella socio-sanitaria Zucchetti Healthcare	-	Dipendenti	Dati comuni, dati particolari, dati giudiziari	INPS, INAIL, Consulente del lavoro, Medico competente, RSPP, Banche, Assicurazioni, Organizzazioni sindacali, Portale PerlaPA, Altri consulenti	Accatre STP (Consulente del lavoro - nomina del 07.02.2024) Halley Veneto Srl (software gestionale – nomina del 25.11.2022) NEXT.ORG Srls (Amministratore di sistema – nomina del 15.11.2021) Zucchetti Healthcare (sw socio-sanitario – nomina del 20.12.2022) Axera SpA (caselle e-mail – nomina del 14.01.2022) Accatre Srl (conservazione sostitutiva – nomina del 25.11.2022)	-	-	Permanente per i dati contenuti nel fascicolo personale 5 anni per i dati relativi alle presenze	Protezione degli accessi logici, Designazione degli incaricati al trattamento, Formazione degli incaricati, Protezione degli accessi fisici, Minimizzazione dei dati trattati, Nomina dei RTD, Backup dei dati, Firewall di rete, Software antivirus, Impianto antincendio	-	-	-
Servizio Segreteria e Protocollo	**Gestione degli amministratori – Consiglio di Amministrazione**	Gestione amministrativa degli amministratori nominati dal Sindaco	Obbligo legale (art. 6, comma 1, lett. c, del GDPR) Esecuzione di un compito di interesse pubblico (art. 6, comma 1, lett. e, del GDPR)	-	Trattamento autorizzato da norme di legge (art. 10 del GDPR e art. 2-octies, comma 3, lett. a, del D.Lgs. 196/2003)	File server in rete, caselle e-mail, Halley	-	Membri del CdA	Dati comuni	Diffusione (per obblighi di trasparenza amministrativa)	NEXT.ORG Srls (Amministratore di sistema – nomina del 15.11.2021) Halley Veneto Srl (software gestionale – nomina del 25.11.2022) Axera SpA (caselle e-mail – nomina del 14.01.2022) Accatre Srl (conservazione sostitutiva – nomina del 25.11.2022)	-	-	Indeterminato fino ad eventuale scarto d'archivio	Protezione degli accessi logici, Designazione degli incaricati al trattamento, Formazione degli incaricati, Protezione degli accessi fisici, Minimizzazione dei dati trattati, Nomina dei RTD, Backup dei dati, Firewall di rete, Software antivirus, Impianto antincendio	-	-	-
Servizio Segreteria e Protocollo	**Gestione dei volontari**	Gestione amministrativa dei volontari	Esecuzione di un contratto (art. 6, comma 1, lett. b, del GDPR) Obbligo legale (art. 6, comma 1, lett. c, del GDPR)	-	-	File server in rete, caselle e-mail, Halley	-	Volontari che operano a favore del centro servizi	Dati comuni	-	NEXT.ORG Srls (Amministratore di sistema – nomina del 15.11.2021) Halley Veneto Srl (software gestionale – nomina del 25.11.2022) Axera SpA (caselle e-mail – nomina del 14.01.2022) Accatre Srl (conservazione sostitutiva – nomina del 25.11.2022)	-	-	Indeterminato fino ad eventuale scarto d'archivio	Protezione degli accessi logici, Designazione degli incaricati al trattamento, Formazione degli incaricati, Protezione degli accessi fisici, Minimizzazione dei dati trattati, Nomina dei RTD, Backup dei dati, Firewall di rete, Software antivirus, Impianto antincendio			
Servizio Segreteria e Protocollo	**Gestione di tirocinanti/stagisti**	Gestione amministrativa dei tirocinanti/stagisti	Esecuzione di un contratto (art. 6, comma 1, lett. b, del GDPR)	-	-	File server in rete, caselle e-mail, Halley	-	Tirocinanti	Dati comuni	Promotori del progetto	NEXT.ORG Srls (Amministratore di sistema – nomina del 15.11.2021) Halley Veneto Srl (software gestionale – nomina del 25.11.2022) Axera SpA (caselle e-mail – nomina del 14.01.2022) Accatre Srl (conservazione sostitutiva – nomina del 25.11.2022)	-	-	Indeterminato fino ad eventuale scarto d'archivio	Protezione degli accessi logici, Designazione degli incaricati al trattamento, Formazione degli incaricati, Protezione degli accessi fisici, Minimizzazione dei dati trattati, Nomina dei RTD, Backup dei dati, Firewall di rete, Software antivirus, Impianto antincendio			
Direzione	**Gestione delle segnalazioni interne da Whistleblowing**																	
Servizio Appalti e Contratti	**Gestione dei fornitori esterni (appalti o incarichi professionali)**	Gestione amministrativa dei fornitori	Esecuzione di un contratto (art. 6, comma 1, lett. b, del GDPR) Obbligo legale (art. 6, comma 1, lett. c, del GDPR)	-	Trattamento autorizzato da norme di legge (art. 10 del GDPR e art. 2-octies, comma 3, lett. a, del D.Lgs. 196/2003)	File server in rete, caselle e-mail, Halley, portale HRMS, cartella socio-sanitaria Zucchetti Healthcare	-	Fornitori e professionisti	Dati comuni, dati giudiziari	Banche ed altri enti pubblici	NEXT.ORG Srls (Amministratore di sistema – nomina del 15.11.2021) Halley Veneto Srl (software gestionale – nomina del 25.11.2022) Zucchetti Healthcare (sw socio-sanitario – nomina del 20.12.2022) Axera SpA (caselle e-mail – nomina del 14.01.2022)	-	-	Indeterminato fino ad eventuale scarto d'archivio	Protezione degli accessi logici, Designazione degli incaricati al trattamento, Formazione degli incaricati, Protezione degli accessi fisici, Minimizzazione dei dati trattati, Nomina dei RTD, Backup dei dati, Firewall di rete, Software antivirus, Impianto antincendio	-	-	-
Diverse	**Gestione degli ospiti (residenziali e semi-residenziali)**	Gestione amministrativa e socio-sanitaria	Esecuzione di un contratto (art. 6, comma 1, lett. b, del GDPR) Obbligo legale (art. 6, comma 1, lett. c, del GDPR)	Diagnosi, assistenza, terapia sanitaria e sociale (art. 9, comma 2, lett. h, del GDPR) Interesse pubblico rilevante (art. 9, comma 2, lett. g, del GDPR e art. 2-sexies, comma 2, lett. s-u, del D.Lgs. 196/2013) Esercitare un diritto in sede giudiziaria (art. 9, comma 2, lett. f, del GDPR)	Trattamento autorizzato da norme di legge (art. 10 del GDPR e art. 2-octies, comma 3, lett. a, del D.Lgs. 196/2003)	File server in rete, caselle e-mail, cartella socio-sanitaria Zucchetti Healthcare	-	Ospiti del centro servizi e del centro diurno	Dati comuni (comprese le foto di riconoscimento presenti nella Cartella Socio Sanitaria), dati particolari, dati giudiziari	Servizio Sanitario Nazionale, Banche	NEXT.ORG Srls (Amministratore di sistema – nomina del 15.11.2021), Zanarotti Donato Giuseppe (Medico – nomina del 01.04.2025), Altri professionisti sanitari Pevarello Stefano (logopedista – nomina del 31.12.2024) Zucchetti Healthcare (sw socio-sanitario – nomina del 20.12.2022) Axera SpA (caselle e-mail – nomina del 14.01.2022)	-	-	Permanente per la cartella sanitaria 10 anni per i dati relativi alla fatturazione Altro: Indeterminato fino ad eventuale scarto d'archivio	Protezione degli accessi logici, Designazione degli incaricati al trattamento, Formazione degli incaricati, Protezione degli accessi fisici, Minimizzazione dei dati trattati, Nomina dei RTD, Backup dei dati, Firewall di rete, Software antivirus, Impianto antincendio			
Diverse	**Gestione delle persone di riferimento, degli amministratori di sostegno, tutori o curatori**	Gestione amministrativa delle persone di riferimento	Esecuzione di un contratto (art. 6, comma 1, lett. b, del GDPR) Obbligo legale (art. 6, comma 1, lett. c, del GDPR) Legittimo interesse del titolare (art. 6, comma 1, lett. F, del GDPR)	-	-	File server in rete, caselle e-mail, cartella socio-sanitaria Zucchetti Healthcare	-	Persone di riferimento degli ospiti (familiari, amministratori di sostegno, tutori, …)	Dati comuni	Studi legali	NEXT.ORG Srls (Amministratore di sistema – nomina del 15.11.2021) Halley Veneto Srl (software gestionale – nomina del 25.11.2022) Zucchetti Healthcare (sw socio-sanitario – nomina del 20.12.2022) Axera SpA (caselle e-mail – nomina del 14.01.2022)	-	-	Indeterminato fino ad eventuale scarto d'archivio	Protezione degli accessi logici, Designazione degli incaricati al trattamento, Formazione degli incaricati, Protezione degli accessi fisici, Minimizzazione dei dati trattati, Nomina dei RTD, Backup dei dati, Firewall di rete, Software antivirus, Impianto antincendio			

Servizi sociali e alberghieri	**Progetto “Take me home”**	Gestione dell’assistenza domiciliare a seguito di dimissioni ospedaliere	Esecuzione di un contratto (art. 6, comma 1, lett. b, del GDPR) Obbligo legale (art. 6, comma 1, lett. c, del GDPR) Legittimo interesse del titolare (art. 6, comma 1, lett. F, del GDPR)	Interesse pubblico rilevante (art. 9, comma 2, lett. g, del GDPR e art. 2-sexies, comma 2, lett. s, del D.Lgs. 196/2013) Esercitare un diritto in sede giudiziaria (art. 9, comma 2, lett. f, del GDPR)	-	File server in rete, caselle e-mail	Comune di Thiene, Istituzione “Villa Miari”, IPAB “La Casa”, IPAB “Muzan”, IPAB “A. Rossi” (accordo stipulato in data 21.11.2024)	Utenti destinatari del servizio di SAD post ricovero	Dati comuni, dati particolari (origine raziale/etnica, convinzioni religiose, relativi alla salute)	-	NEXT.ORG Srls (Amministratore di sistema – nomina del 15.11.2021) Halley Veneto Srl (software gestionale – nomina del 25.11.2022) Axera SpA (caselle e-mail – nomina del 14.01.2022) Bassano solidale Soc. Coop. – nomina del 07.12.2020) Accatre Srl (conservazione sostitutiva – nomina del 25.11.2022)	-	-	Indeterminato fino ad eventuale scarto d’archivio	Protezione degli accessi logici, Designazione degli incaricati al trattamento, Formazione degli incaricati, Protezione degli accessi fisici, Minimizzazione dei dati trattati, Nomina dei RTD, Backup dei dati, Firewall di rete, Software antivirus, Impianto antincendio			
Diverse	**Attività promozionali dell’ente**	Attività promozionali dell’ente	Consenso al trattamento dei propri dati personali per una o più specifiche finalità (art. 6, comma 1, lett. a, del GDPR)	-	-	Pubblicazioni cartacee, sito internet istituzionale	-	Dipendenti, amministratori, ospiti del centro servizi, ospiti del centro diurno, volontari	Dati comuni (foto, video)	Diffusione	Halley Veneto Srl (Gestore sito internet – nomina del 25.11.2022)	-	-	Indeterminato fino ad eventuale scarto d’archivio	Protezione degli accessi logici, Designazione degli incaricati al trattamento, Formazione degli incaricati, Protezione degli accessi fisici, Minimizzazione dei dati trattati, Nomina dei RTD, Backup dei dati, Firewall di rete, Software antivirus, Impianto antincendio			

Trattamenti effettuati in qualità di RESPONSABILE del trattamento

Registro dei trattamenti

Unità Organizzativa	Denominazione e dati di contatto del TITOLARE	Denominazione e dati di contatto del Rappresentante del Titolare	Denominazione e dati di contatto del Responsabile della protezione dei dati (DPO)	Denominazione del trattamento	Categoria dei trattamenti	Paesi Terzi o organizzazioni internazionali verso cui i dati possono essere trasferiti	Indicazione delle garanzie adottate per il trasferimento internazionale	Descrizione generale delle misure di sicurezza adottate	Riferimento all'accordo scritto con il Titolare
Servizi sociali	**Comune di Valdastico**	-	info@in4data.it	Gestione del servizio SAD	Conservazione, modifica, estrazione, consultazione, uso, comunicazione	-	-	Protezione degli accessi logici, Designazione degli incaricati al trattamento, Formazione degli incaricati, Protezione degli accessi fisici, Minimizzazione dei dati trattati, Nomina dei RTD, Backup dei dati, Firewall di rete, Software antivirus, Impianto antincendio	Accordo sottoscritto in data 02.10.2023
Servizi sociali	**Comune di Valdastico**	-	info@in4data.it	Consegna a domicilio dei pasti caldi	Conservazione, modifica, estrazione, consultazione, uso, comunicazione	-	-	Protezione degli accessi logici, Designazione degli incaricati al trattamento, Formazione degli incaricati, Protezione degli accessi fisici, Minimizzazione dei dati trattati, Nomina dei RTD, Backup dei dati, Firewall di rete, Software antivirus, Impianto antincendio	Accordo sottoscritto in data 02.10.2023
Servizio Segreteria e Protocollo	**Azienda ULSS n. 7 "Pedemontana"**	-	rpd@aulss7.veneto.it	Gestione degli ospiti del centro servizi e delle relativi impegnative di residenzialità	Conservazione, modifica, estrazione, consultazione, uso, comunicazione	-	-	Protezione degli accessi logici, Designazione degli incaricati al trattamento, Formazione degli incaricati, Protezione degli accessi fisici, Minimizzazione dei dati trattati, Nomina dei RTD, Backup dei dati, Firewall di rete, Software antivirus, Impianto antincendio	Accordo sottoscritto in data 30.07.2024

fettuati in qualità di RESPONSABILE del trattamento

Registro dei trattamenti

Denominazione e dati di contatto del TITOLARE	Denominazione e dati di contatto del Rappresentante del Titolare	Denominazione e dati di contatto del Responsabile della protezione dei dati (DPO)	Denominazione del trattamento	Categoria dei trattamenti	Paesi Terzi o organizzazioni internazionali verso cui i dati possono essere trasferiti	Indicazione delle garanzie adottate per il trasferimento internazionale	Descrizione generale delle misure di sicurezza adottate	Riferimento all'accordo scritto con il Titolare	Denominazione dei sub-responsabili	Effettuazione di una valuta del Tit
Comune di Valdastico	-	info@in4data.it	Gestione del servizio SAD	Conservazione, modifica, estrazione, consultazione, uso, comunicazione	-	-	Protezione degli accessi logici, Designazione degli incaricati al trattamento, Formazione degli incaricati, Protezione degli accessi fisici, Minimizzazione dei dati trattati, Nomina dei RTD, Backup dei dati, Firewall di rete, Software antivirus, Impianto antincendio	Accordo sottoscritto in data 02.10.2023	Bassano Solidale soc.coop.soc. Axera SpA Halley Veneto Srl Accatre Srl	NO
Comune di Valdastico	-	info@in4data.it	Consegna a domicilio dei pasti caldi	Conservazione, modifica, estrazione, consultazione, uso, comunicazione	-	-	Protezione degli accessi logici, Designazione degli incaricati al trattamento, Formazione degli incaricati, Protezione degli accessi fisici, Minimizzazione dei dati trattati, Nomina dei RTD, Backup dei dati, Firewall di rete, Software antivirus, Impianto antincendio	Accordo sottoscritto in data 02.10.2023	Bassano Solidale soc.coop.soc. Axera SpA Halley Veneto Srl Accatre Srl	NO
Azienda ULSS n. 7 “Pedemontana”	-	rpd@aulss7.veneto.it	Gestione degli ospiti del centro servizi e delle relativi impegnative di residenzialità	Conservazione, modifica, estrazione, consultazione, uso, comunicazione	-	-	Protezione degli accessi logici, Designazione degli incaricati al trattamento, Formazione degli incaricati, Protezione degli accessi fisici, Minimizzazione dei dati trattati, Nomina dei RTD, Backup dei dati, Firewall di rete, Software antivirus, Impianto antincendio	Accordo sottoscritto in data 30.07.2024	NEXT.ORG, Zucchetti Healthcare Srl, AXERA, Halley Veneto Srl	NO

Potenziale violazione di dati personali

Modello di comunicazione al Direttore

Cognome e nome del segnalante: _____

Breve descrizione della violazione dei dati personali

Denominazione della/e banche dati oggetto di *data breach* e breve descrizione della violazione dei dati personali ivi trattati

Quando si è verificata la violazione dei dati personali trattati nell'ambito della banca dati?

- ☐ Il _____
- ☐ Tra il _____ e il _____
- ☐ In un tempo non ancora determinato
- ☐ È possibile che sia ancora in corso

Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

Modalità di esposizione al rischio: tipo di violazione

- ☐ Lettura (presumibilmente i dati non sono stati copiati)
- ☐ Copia (i dati sono ancora presenti sui sistemi del titolare)
- ☐ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
- ☐ Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
- ☐ Furto (i dati non sono più sui sistemi del titolare ma sono in possesso dell'autore della violazione)
- ☐ Altro _____

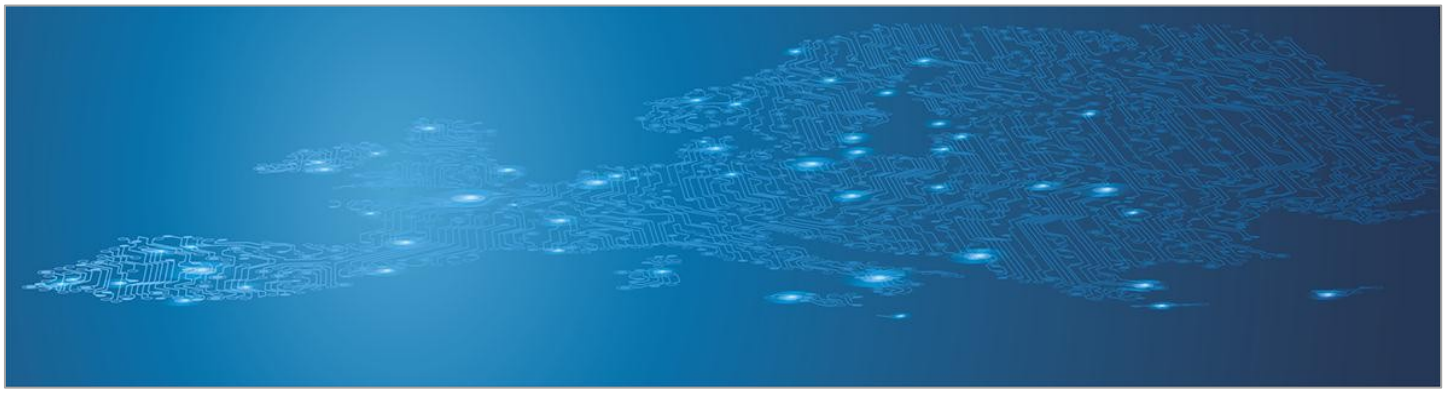
Dispositivo o strumento oggetto della violazione

☐ Computer ☐ Rete ☐ Dispositivo mobile ☐ File o parte di file ☐ Strumento di backup	☐ Documento cartaceo ☐ Softwre _____ ☐ Servizio informatico _____ ☐ Altro _____

Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati?

- ☐ Numero _____ di persone
- ☐ Circa _____ persone
- ☐ Un numero (ancora) sconosciuto di persone

Data, _____ Firma del segnalante



Raccomandazioni
per una metodologia di valutazione della gravità delle violazioni dei dati personali

Documento di lavoro, v1.0, dicembre 2013

Agenzia dell'Unione Europea per la sicurezza delle reti e dell'informazione

www.enisa.europa.eu

Informazioni sull'ENISA

L'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) è un centro di competenza in materia di sicurezza delle reti e dell'informazione per l'UE, i suoi Stati membri, il settore privato e i cittadini europei. L'ENISA collabora con questi gruppi per sviluppare consigli e raccomandazioni sulle buone pratiche in materia di sicurezza delle informazioni. Assiste gli Stati membri dell'UE nell'attuazione della legislazione comunitaria in materia e lavora per migliorare la resilienza delle infrastrutture informatiche e delle reti critiche europee. L'ENISA cerca d i valorizzare le competenze esistenti negli Stati membri dell'UE sostenendo lo sviluppo di comunità transfrontaliere impegnate a migliorare la sicurezza delle reti e delle informazioni in tutta l'UE. Ulteriori informazioni sull'ENISA e sul suo lavoro sono disponibili sul sito www.enisa.europa.eu.

Gli autori

Questo documento è stato prodotto dagli esperti delle Autorità per la protezione dei dati personali di Grecia e Germania in collaborazione con l'ENISA.

Redattori

Clara Galan Manso (Esperto nazionale distaccato) Sławomir Górniak

Contatto

Per contattare gli autori si prega di utilizzare sta@enisa.europa.eu

Per le richieste dei media su questo articolo, si prega di utilizzare il **sito**press@enisa.europa.eu **.**

Ringraziamenti

Desideriamo ringraziare i rappresentanti delle autorità di protezione dei dati che partecipano al sottogruppo tecnologico del Gruppo di lavoro articolo 29 per il loro prezioso feedback che ci aiuterà a migliorare ulteriormente la metodologia. Desideriamo inoltre ringraziarli per la presentazione di casi di prova che ci hanno aiutato a valutare l'efficacia della metodologia.

ISBN: 978-92-9204-078-9 DOI: 10.2824/27590

Acronimi

Art.29 WP - Gruppo di lavoro per la tutela delle persone fisiche con riguardo al trattamento dei dati personali

CB - Circostanze della violazione

DC - Titolare del trattamento dei dati

DPA - Data Protection Authority **DPO** - Data Protection Officer **DPC** - Data processing context **EI** - Ease of identification (facilità di identificazione)

ENISA - Agenzia dell'Unione Europea per la sicurezza delle reti e dell'informazione

TS - Sottogruppo Tecnologia (del Gruppo di lavoro Art.29)

Sintesi

L'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) ha esaminato le misure e le procedure esistenti negli Stati membri dell'UE in materia di violazione dei dati personali e ha pubblicato nel 2011 uno studio sull'attuazione tecnica dell'articolo 4 dell'ePrivacy. 4 della Direttiva ePrivacy, che includeva raccomandazioni su come pianificare e preparare le violazioni dei dati, come rilevarle e valutarle, come notificarle alle persone e alle autorità competenti e come rispondere alle violazioni dei dati. In allegato alle suddette raccomandazioni è stata inclusa anche una proposta di metodologia per la valutazione della gravità delle violazioni dei dati personali, che tuttavia non è stata ritenuta sufficientemente matura per essere utilizzata a livello nazionale dalle diverse autorità di protezione dei dati.

In questo contesto, le Autorità per la protezione dei dati di Grecia e Germania, in collaborazione con l'ENISA, hanno sviluppato, sulla base del lavoro sopra menzionato, una metodologia aggiornata per la valutazione della gravità delle violazioni dei dati che potrebbe essere utilizzata sia dalle autorità per la protezione dei dati che dai responsabili del trattamento. Questo documento di lavoro è un primo risultato della collaborazione tra gli esperti delle due DPA e dell'ENISA. Si prevede di sviluppare ulteriormente la metodologia con l'obiettivo di generare uno strumento pratico finale per la valutazione della gravità della violazione dei dati.

Una panoramica della metodologia proposta è presentata nella sezione 2 del presente documento e ulteriormente elaborata nelle sezioni successive. La gravità di una violazione è definita come la stima dell'entità dell'impatto potenziale sugli individui derivante dalla violazione dei dati. Gli elementi fondamentali che devono essere presi in considerazione per valutare tale gravità sono:

- Contesto di elaborazione dei dati - il tipo di dati violati è adattato al contesto in cui vengono utilizzati.
- facilità di identificazione dell'individuo in base ai dati violati
- Circostanze della violazione, che hanno un'ulteriore influenza sulla gravità di una violazione.

La metodologia presentata in questo studio si basa su un approccio il più possibile oggettivo, pur essendo sufficientemente flessibile da poter essere adottata da diverse autorità di protezione dei dati, adattandola alle loro dimensioni, al sistema giuridico nazionale e ad altri fattori. In base alle diverse esigenze, il punteggio di alcune categorie può essere modificato per produrre i risultati più appropriati.

Indice dei contenuti

1 Introduzione

1.1 Informazioni di base

Con la modifica della Direttiva 2002/58/CE[1] (Direttiva ePrivacy) è stato introdotto l'obbligo di notifica delle violazioni dei dati personali da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico alle autorità competenti e alle persone interessate (art. 4). La Commissione europea, come previsto dalla direttiva, ha pubblicato misure di attuazione riguardanti principalmente il formato e le circostanze della notifica delle violazioni dei dati personali - Regolamento (UE) n. 611/2013 della Commissione[2].

A seguito delle disposizioni della Direttiva ePrivacy, nella bozza di Regolamento sulla protezione dei dati personali (art. 31) è stata introdotta una proposta di obbligo generale di notifica delle violazioni dei dati personali da parte dei titolari del trattamento a determinate condizioni, nel contesto del pacchetto complessivo di riforma della protezione dei dati[3].

Entrambe le disposizioni legislative costituiscono un importante sviluppo che ha il potenziale di aumentare il livello di sicurezza dei dati in Europa e di rassicurare i cittadini sul modo in cui i loro dati personali sono garantiti e protetti dai responsabili del trattamento. Nell'ambito dell'effettiva attuazione dell'obbligo di notifica delle violazioni dei dati, il Gruppo di lavoro "Articolo 29" ha concluso, attraverso i suoi sottogruppi "ePrivacy" e "Tecnologia", che vi è una seria necessità di sviluppare una metodologia per la valutazione della gravità delle violazioni dei dati personali. Le discussioni all'interno del Gruppo di lavoro Articolo 29 sono attualmente ancora in corso.

L'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) ha esaminato le misure e le procedure già esistenti negli Stati membri dell'UE in materia di violazioni dei dati personali e ha pubblicato nel 2011 un rapporto sull'attuazione tecnica dell'articolo 4 della direttiva ePrivacy. 4 della Direttiva ePrivacy[4]. In allegato a tale relazione è stata inclusa una proposta di metodologia per la valutazione della gravità delle violazioni dei dati personali, che tuttavia non è stata ritenuta sufficientemente matura per essere utilizzata a livello nazionale dalle diverse autorità di protezione dei dati.

In questo contesto, le Autorità per la protezione dei dati di Grecia e Germania, in collaborazione con l'ENISA, hanno sviluppato, sulla base del lavoro sopra menzionato, una metodologia aggiornata per la valutazione della gravità delle violazioni dei dati che potrebbe essere utilizzata sia dalle autorità per la protezione dei dati che dai responsabili del trattamento. Questo documento di lavoro è un primo risultato della collaborazione tra gli esperti delle due DPA e dell'ENISA. Si prevede di sviluppare ulteriormente la metodologia con l'obiettivo di generare uno strumento pratico finale per la valutazione della gravità della violazione dei dati.

1.2 Obiettivi

La metodologia proposta e presentata in questo documento è stata concepita con i seguenti obiettivi:

- Fornire ai responsabili del trattamento dei dati uno strumento quantitativo (nella misura in cui ciò sia possibile) per valutare la gravità delle violazioni dei dati e notificare di conseguenza le autorità competenti e le autorità di controllo.

[1] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:01:EN:HTML
[2] http://eur-lex.europa.eu/JOHtml.do?uri=OJ:L:2013:173:SOM:EN:HTML
[3] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
[4] Raccomandazioni sulle linee guida per l'attuazione tecnica dell'articolo 4, http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/dbn/art4_tech

i n t e r e s s a t i . Lo strumento potrebbe anche servire ai responsabili del trattamento per determinare rapidamente le misure di attenuazione necessarie.

- Fornire alle autorità nazionali competenti uno strumento per valutare la gravità delle violazioni notificate dai responsabili del trattamento.

- Supportare le autorità nazionali competenti nell'esecuzione di analisi e statistiche dettagliate sulle violazioni dei dati personali segnalate.

- Contribuire all'armonizzazione della valutazione della gravità delle violazioni dei dati personali nell'Unione Europea, proponendo una metodologia comune e un punteggio di gravità. Ciò sarebbe particolarmente importante nel caso di violazioni transfrontaliere.

1.3 Gravità delle violazioni di dati

La gravità di una violazione di dati personali è definita, nel contesto di questa metodologia, come la ***"stima dell'entità dell'impatto potenziale sulle persone derivante dalla violazione dei dati"***.

Come stabilito nella Direttiva 2009/136/CE[5] (considerando (61)), l'impatto di una violazione di dati personali può includere "ad esempio, furto di identità o frode, danni fisici, umiliazioni significative o danni alla reputazione in relazione alla fornitura di servizi di comunicazione accessibili al pubblico nella Comunità".

Con l'utilizzo di questa metodologia, il titolare del trattamento è guidato nel processo da specifici criteri quantitativi per effettuare la valutazione complessiva. Gli stessi criteri possono essere utilizzati dalle autorità competenti, insieme alle informazioni fornite dal responsabile del trattamento nel modulo di notifica[6], per effettuare la propria valutazione della violazione.

Va notato che il responsabile del trattamento applica la metodologia utilizzando le informazioni in suo possesso al momento della violazione. In tal senso, la metodologia non può sempre coprire tutte le possibili casistiche, compresi i probabili impatti su gruppi specifici di individui o casi molto particolari che non possono essere affrontati pienamente nell'ambito di una metodologia generale. Pertanto, va ricordato che sia i responsabili del trattamento dei dati che le autorità competenti devono prestare particolare attenzione quando si tratta di casi che, a causa delle loro specificità, non possono essere valutati correttamente con questa metodologia.

[5] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF
[6] Un esempio di modello di modulo di notifica di violazione dei dati alle autorità competenti è disponibile nell'Appendice A di http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/dbn/art4_tech.

2 Panoramica della metodologia

2.1 Criteri

I principali criteri presi in considerazione per valutare la gravità di una violazione di dati personali sono:

- **Contesto del trattamento dei dati (DPC):** Si occupa del tipo di dati violati, insieme a una serie di fattori legati al contesto generale del trattamento.
- **Facilità di identificazione (EI):** Determina la facilità con cui l'identità delle persone può essere dedotta dai dati coinvolti nella violazione.
- **Circostanze della violazione (CB):** Si occupa delle circostanze specifiche della violazione, che sono legate al tipo di violazione, tra cui principalmente la perdita di sicurezza dei dati violati, nonché qualsiasi intento doloso coinvolto.

2.2 Calcolo della gravità

Sulla base dei criteri di cui sopra, l'approccio di questa metodologia è il seguente:

- Il DPC è il fulcro della metodologia e valuta la criticità di un determinato set di dati in uno specifico contesto di elaborazione.
- L'EI è un fattore di correzione del DPC. La criticità complessiva di un'elaborazione di dati può essere ridotta in base al valore di EI. In altre parole, minore è la facilità di identificazione, minore è il punteggio complessivo. Pertanto, la combinazione di EI e DPC (moltiplicazione) fornisce il punteggio iniziale della gravità (SE) della violazione dei dati.
- Il CB quantifica le circostanze specifiche della violazione che possono essere presenti o meno in una particolare situazione. Pertanto, quando è presente, il CB può solo aumentare la gravità di una specifica violazione. Per questo motivo il punteggio iniziale può essere ulteriormente modificato dalla BC.

Pertanto, il punteggio finale della valutazione della gravità può essere estratto utilizzando la seguente formula:

$$SE = DPC \times EI + CB$$

In questo modo, affinché il controllore ottenga il risultato di gravità, tutti e tre i criteri devono essere valutati.

Il risultato appartiene a un certo intervallo di valori che corrisponde a uno dei quattro livelli di gravità: basso, medio, alto e molto alto[7]. Al termine della valutazione, vengono valutati altri criteri eventualmente rilevanti (numero di individui e incomprensibilità dei dati) che non sono stati presi in considerazione nella metodologia e segnalati all'autorità competente, se del caso.

È essenziale tenere presente che tutti i punteggi e/o le classifiche utilizzati in questa metodologia sono stati stabiliti esclusivamente per l'uso all'interno della formula di gravità. Non sono destinati ad avere alcun significato per una conclusione sulla ponderazione o sulla classificazione di certi tipi di dati in generale, né tanto meno per un'indicazione di eventuali conseguenze legali o precedenti sull'uso di questi dati per altri scopi.

[7] I livelli di gravità saranno spiegati in dettaglio nella sezione 3.2.

3 Descrizione dettagliata dei punteggi e dei livelli di gravità

3.1 Punteggio dei criteri

3.1.1 Contesto di elaborazione dei dati (DPC)

Per definire il punteggio per il DPC, il titolare del trattamento deve seguire le fasi successive:

- Fase 1: Definizione e classificazione dei tipi di dati personali

  a) Definire i tipi di dati personali coinvolti nella violazione.

  b) Classificare i dati in almeno una delle quattro categorie: dati semplici, comportamentali, finanziari e sensibili (queste categorie sono spiegate in dettaglio nell'Allegato 1). In questo modo si ottiene un punteggio DPC di base preliminare.

  L'elenco dei tipi di dati descritti nelle quattro categorie non è esaustivo; tuttavia, la maggior parte dei dati coinvolti in casi reali può essere abbinata ad almeno una delle categorie. Le credenziali non sono considerate una categoria di dati specifica e devono essere gestite in base al tipo di dati elaborati dai sistemi a cui forniscono accesso.

- Fase 2: Adattamento in base a fattori contestuali legati al trattamento dei dati

  c) Valutare la presenza di alcuni fattori che potrebbero aumentare o diminuire il punteggio di base (volume dei dati, caratteristiche particolari dei responsabili del trattamento o delle persone, invalidità/accuratezza dei dati, disponibilità pubblica (prima della violazione), natura dei dati).

  d) Nel caso in cui esistano tali fattori, aumentare/diminuire di conseguenza il punteggio di base. La Tabella di valutazione 1 fornisce le scale di aggiustamento per categoria di dati, insieme a casi esemplificativi che potrebbero portare a punteggi più bassi o più alti.

Si rimanda all'Allegato 1 per un elenco di fattori contestuali ed esempi specifici di punteggio DPC.

Nota: anche se, ai fini della metodologia, vengono classificate quattro categorie di dati, la categorizzazione in sé non deve essere vista come una classifica generale dei tipi di dati in questione. Inoltre, per quanto riguarda il trattamento di un certo tipo di dati, è sempre necessario prendere in considerazione ulteriori fattori contestuali relativi ai dati. Pertanto, il punteggio di base deve essere visto solo come un'indicazione generale della criticità connessa a una determinata categoria di dati e il punteggio DPC di qualsiasi tipo di dati può sempre variare da 1 a 4.

Se i dati corrispondono a più di una categoria, i passaggi sopra descritti devono essere seguiti per ogni categoria applicabile. In questi casi il valore da utilizzare per il calcolo complessivo della gravità sarà il punteggio più alto raggiunto.

Se il responsabile del trattamento sceglie di modificare il punteggio di base del DPC (entro l'intervallo della tabella di valutazione 1), il nuovo punteggio deve essere supportato da una spiegazione che descriva i particolari fattori contestuali della violazione e la loro influenza.

3.1.2 Facilità di identificazione (EI)

La facilità di identificazione (EI) valuta la facilità con cui un soggetto che ha accesso all'insieme di dati p u ò associarli univocamente a una determinata persona.

Ai fini di questa metodologia abbiamo definito quattro livelli di EI (trascurabile, limitato, significativo e massimo) con un incremento lineare del punteggio. Il punteggio più basso viene assegnato quando la possibilità di identificare l'individuo è trascurabile, il che significa che è estremamente difficile associare i dati a una determinata persona, ma potrebbe comunque essere possibile in determinate condizioni. Il punteggio più alto viene scelto quando l'identificazione è possibile direttamente dai dati violati, senza che siano necessarie ricerche particolari per scoprire l'identità dell'individuo. L'Allegato 2 descrive questi livelli in dettaglio.

Nel definire l'EI, occorre tenere conto del fatto che l'identificazione può essere possibile direttamente (ad esempio, sulla base di un nome) o indirettamente (ad esempio, sulla base di un numero di identificazione) dai dati violati, ma può anche dipendere dal contesto specifico della violazione. Pertanto, alcuni identificatori possono portare a punteggi EI diversi a seconda del caso specifico della violazione.

Si rimanda all'Allegato 2 per esempi specifici di attribuzione di EI utilizzando identificatori comuni.

Inoltre, nel definire le IE il responsabile del trattamento deve tenere conto di tutti i mezzi che possono essere ragionevolmente utilizzati da chiunque per identificare le persone. Ciò include le informazioni pubbliche, detenute o ottenute in altro modo, anche tramite Internet, nonché la possibile corrispondenza incrociata con altre fonti a cui il titolare del trattamento o una terza parte possono accedere.

3.1.3 Circostanze della violazione (CB)

Gli elementi che vengono considerati nell'ambito del CB sono la perdita di sicurezza (riservatezza, integrità, disponibilità) e l'intento doloso e sono complementari al DPC e all'EI, come segue:

Perdita di riservatezza: La perdita di riservatezza si verifica quando le informazioni sono accessibili a soggetti non autorizzati o che non hanno uno scopo legittimo per accedervi. L'entità della perdita di riservatezza varia in base alla portata della divulgazione, ossia al numero e al tipo di soggetti che possono accedere illegalmente alle informazioni.

Perdita di integrità: La perdita di integrità si verifica quando l'informazione originale viene alterata e la sostituzione dei dati può essere pregiudizievole per l'individuo. La situazione più grave si verifica quando ci sono serie possibilità che i dati alterati siano stati utilizzati in modo da danneggiare l'individuo.

Perdita di disponibilità: La perdita di disponibilità si verifica quando non è possibile accedere ai dati originali quando se ne ha bisogno. Può essere temporanea (i dati sono recuperabili, ma ci vorrà un certo periodo di tempo e questo può essere dannoso per l'individuo) o permanente (i dati non possono essere recuperati).

Intenzione dolosa: Questo elemento esamina se la violazione è dovuta a un errore o a un errore, umano o tecnico, o se è stata causata da un'azione intenzionale con intento doloso. Le violazioni non dolose comprendono i casi di perdita accidentale, smaltimento inadeguato, errore umano e bug o errata configurazione del software. Le violazioni dolose comprendono i casi di furto e hacking che mirano a danneggiare le persone (ad esempio, esponendo i loro dati personali a terzi non autorizzati). In altri casi, l'intento doloso potrebbe includere il trasferimento di dati personali a terzi a scopo di lucro (ad esempio, la vendita di elenchi di dati personali). In alcuni casi l'intento doloso può essere dedotto anche da azioni che mirano a danneggiare il titolare del trattamento (ad esempio, rubando ed esponendo i dati personali a terzi non autorizzati). L'intento doloso è un fattore che aumenta la probabilità che i dati vengano utilizzati in modo dannoso, poiché questo era lo scopo iniziale della violazione.

Per quanto riguarda il punteggio delle BC, a differenza di DPC e EI in cui si sceglie il punteggio massimo raggiungibile, i punti ottenuti per ogni elemento della BC vengono sommati per ottenere il punteggio finale, poiché nella stessa violazione possono verificarsi circostanze diverse. La Tabella di valutazione 3 fornisce punteggi diversi per ogni elemento CB e per i diversi tipi di circostanze.

Si rimanda all'Allegato 3 per esempi specifici di punteggio per le BC.

3.2 Definizione del livello di gravità

Come introdotto nella Sezione 2.2, la gravità complessiva (SE) è calcolata con la seguente formula:

$$SE = DPC \times EI + CB$$

Il punteggio finale indica il livello di gravità di una determinata violazione, tenendo conto dell'impatto sulle persone[8].

Gravità di una violazione dei dati		
SE< 2	Basso	Le persone non saranno colpite o potranno incontrare qualche inconveniente, che supereranno senza problemi (tempo impiegato per reinserire le informazioni, fastidi, irritazioni, ecc.)
2≤ SE< 3	Medio	Le persone possono incontrare disagi significativi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accedere ai servizi commerciali, paura, mancanza di comprensione, stress, piccoli disturbi fisici, ecc.)
3≤ SE< 4	Elevato	Gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento nella lista nera delle banche, danni alla proprietà, perdita del lavoro, citazione in giudizio, peggioramento della salute, ecc.)
4≤ SE	Molto alto	Le persone possono andare incontro a conseguenze significative, o addirittura irreversibili, che non possono essere superate (difficoltà finanziarie come un forte indebitamento o l'impossibilità di lavorare, disturbi psicologici o fisici di lunga durata, morte, ecc.)

3.3 Bandiere

Una volta definito il livello di gravità, questo può essere accompagnato da flag che indicano alcuni elementi della violazione che, pur non influendo a priori sul punteggio, sono importanti per la valutazione finale. Ai fini della metodologia, sono stati considerati due flag:

Numero di individui violati superiore a 100. I dati di un singolo individuo, violati nel contesto di un incidente più grande, possono potenzialmente essere divulgati più facilmente, mentre allo stesso tempo un numero elevato di individui colpiti influenza la portata complessiva della violazione.

Dati incomprensibili. La non intelligibilità (ad esempio, sotto forma di crittografia forte e senza compromissione delle chiavi) può ridurre sostanzialmente l'impatto sulle persone, poiché diminuisce notevolmente la possibilità di accesso ai dati da parte di soggetti non autorizzati.

[8]La tabella che stabilisce i livelli di gravità di una violazione dei dati è stata introdotta per la prima volta nelle "Raccomandazioni sugli orientamenti per l'attuazione tecnica dell'articolo 4", a pagina 24, ma è stata resa più precisa nel presente documento.

4 Uso della metodologia

4.1.1 Notifica alle autorità competenti

Il livello di gravità della violazione (insieme ai flag), calcolato attraverso questa metodologia, potrebbe essere integrato nella notifica inviata dal responsabile del trattamento alle autorità competenti. Ciò può essere fatto automaticamente nel modello di notifica o attraverso l'uso di uno strumento autonomo. Le autorità competenti saranno libere di valutare il risultato (utilizzando lo stesso modello/strumento e le informazioni fornite dal responsabile del trattamento) e di accettarlo o rifiutarlo, in base alla propria valutazione.

Se per qualche motivo il livello di gravità finale è ritenuto errato dal titolare del trattamento, il titolare del trattamento potrebbe indicare il livello "corretto", comprese le proprie argomentazioni per il diverso risultato, in una casella di testo libera (ad esempio, integrata nel modulo di notifica). Inoltre, qualsiasi modifica del punteggio predefinito per il criterio DPC dovrebbe essere spiegata dal responsabile del trattamento utilizzando una casella di testo libero. Queste caselle potrebbero anche essere utilizzate per lasciare commenti senza modificare il livello di gravità.

4.1.2 Notifica alle persone

Il livello di gravità può essere utilizzato dal responsabile del trattamento e dall'autorità competente per determinare se è necessario notificare le persone. Il livello in base al quale la notifica deve essere considerata necessaria potrebbe essere accettato da tutte le autorità competenti o variare in base a criteri nazionali.

5 Osservazioni conclusive

Nelle pagine precedenti abbiamo presentato un documento di lavoro sulla nostra proposta di metodologia per la valutazione delle violazioni dei dati. Questa proposta mira in ultima analisi a essere integrata in un modello di notifica (come nelle Raccomandazioni dell'ENISA per l'attuazione tecnica dell'articolo 4 della Direttiva ePrivacy[9]) per ottenere una valutazione il più possibile automatizzata della gravità.

La metodologia presentata in questo studio si basa su un approccio il più possibile oggettivo, pur essendo sufficientemente flessibile da poter essere adottata da diverse autorità di protezione dei dati, adattandola alle loro dimensioni, al sistema giuridico nazionale e ad altri fattori. In base alle diverse esigenze, il punteggio di alcune categorie può essere modificato per produrre i risultati più appropriati:

- Il contesto del trattamento dei dati può essere regolato in base all'importanza dei dati (semplici, comportamentali, finanziari, ecc.) assegnata dalla specifica autorità di protezione dei dati.
- La facilità di identificazione può tenere conto della realtà di un dato Paese e del suo sistema giuridico (disponibilità pubblica di numeri personali, nomi, indirizzi, ecc.)
- Le circostanze di una violazione offrono la massima flessibilità per adattare il risultato finale alle esigenze di una DPA.
- I flag possono essere modificati (ad esempio in funzione dei record violati), integrati da nuovi o spostati nella tabella CB (circostanze di una violazione).

L'ENISA e le DPA di Grecia e Germania intendono sviluppare ulteriormente il lavoro presentato in questo documento, con l'obiettivo finale di pubblicare uno strumento pratico di gravità delle violazioni dei dati che possa essere utile sia per le DPA che per i responsabili del trattamento dei dati in tutta l'UE.

[9] http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/dbn/art4_tech

Allegato 1 - Contesto del trattamento dei dati

A1 Tabelle di valutazione

Tabella 1: Contesto di elaborazione dei dati (DPC)		Punteggio
Dati semplici	Ad esempio, dati biografici, dettagli di contatto, nome e cognome, dati sull'istruzione, sulla vita familiare, sull'esperienza professionale, ecc.	
	Punteggio di base preliminare: quando la violazione riguarda "dati semplici" e il responsabile del trattamento non è a conoscenza di fattori aggravanti.	**1**
	Il punteggio del DPC potrebbe essere aumentato di 1, ad esempio quando il volume dei "dati semplici" e/o le caratteristiche del responsabile del trattamento sono tali da consentire una certa profilazione dell' individuo o la formulazione di ipotesi sul suo status sociale/finanziario.	2
	Il punteggio del DPC potrebbe essere di 2, ad esempio quando i "semplici dati" e/o le caratteristiche del responsabile del trattamento possono portare a supposizioni sullo stato di salute, sulle preferenze sessuali, sulle convinzioni politiche o religiose dell'individuo.	3
	Il punteggio DPC potrebbe essere aumentato di 3, ad esempio quando, a causa di alcune caratteristiche dell'individuo (ad esempio gruppi vulnerabili, minori), le informazioni possono essere critiche per la sua sicurezza personale o le sue condizioni fisiche/psicologiche.	4
Dati comportamentali	Ad esempio, dati relativi all'ubicazione, al traffico, alle preferenze e alle abitudini personali, ecc.	
	Punteggio preliminare di base: quando la violazione riguarda "dati comportamentali" e il responsabile del trattamento non è a conoscenza di fattori aggravanti o attenuanti.	**2**
	Il punteggio del DPC potrebbe essere diminuito di 1, ad esempio quando la natura dell'insieme di dati non fornisce alcuna visione sostanziale delle informazioni comportamentali dell'individuo o i dati possono essere raccolti facilmente (indipendentemente dalla violazione) attraverso fonti pubblicamente disponibili (ad esempio, combinazione di informazioni provenienti da ricerche sul web).	1
	Il punteggio DPC può essere aumentato di 1, ad esempio quando il volume dei "dati comportamentali" e/o le caratteristiche del responsabile del trattamento sono tali da consentire la creazione di un profilo dell'individuo, esponendo informazioni dettagliate sulla sua vita quotidiana e sulle sue abitudini.	3
	Il punteggio DPC può essere aumentato di 2, ad esempio se è possibile creare un profilo basato sui dati sensibili dell'individuo.	4

Dati finanziari	Qualsiasi tipo di dati finanziari (ad es. reddito, transazioni finanziarie, estratti conto bancari, investimenti, carte di credito, fatture, ecc.) Include i dati sociali relativi alle informazioni finanziarie.	
	Punteggio di base preliminare: quando la violazione riguarda "dati finanziari" e il responsabile del trattamento non è a conoscenza di fattori aggravanti o attenuanti.	**3**
	Il punteggio DPC potrebbe essere diminuito di 2, ad esempio quando la natura del set di dati non fornisce informazioni sostanziali sulle informazioni finanziarie dell'individuo (ad esempio, il fatto che una persona sia cliente di una certa banca senza ulteriori dettagli).	1
	Il punteggio DPC può essere diminuito di 1, ad esempio quando il set di dati specifici include alcune informazioni finanziarie, ma non fornisce alcuna visione significativa dello stato/situazione finanziaria dell'individuo (ad esempio, semplici numeri di conti bancari senza ulteriori dettagli).	2
	Il punteggio DPC potrebbe essere aumentato di 1, ad esempio quando, a causa della natura e/o del volume dello specifico set di dati, vengono divulgate informazioni finanziarie complete (ad esempio, carte di credito) che potrebbero consentire frodi o viene creato un profilo sociale/finanziario dettagliato.	4
Dati sensibili	Qualsiasi tipo di dati sensibili (ad es. salute, affiliazione politica, vita sessuale).	
	Punteggio di base preliminare: quando la violazione riguarda "dati sensibili" e il responsabile del trattamento non è a conoscenza di fattori attenuanti.	**4**
	Il punteggio del DPC potrebbe essere diminuito di 1, ad esempio quando la natura dell'insieme di dati non fornisce alcuna visione sostanziale delle informazioni comportamentali dell'individuo o i dati possono essere raccolti facilmente (indipendentemente dalla violazione) attraverso fonti pubblicamente disponibili (ad esempio, una combinazione di informazioni provenienti da ricerche sul web).	1
	Il punteggio DPC potrebbe essere diminuito di 2, ad esempio quando la natura dei dati può portare a ipotesi generali.	2
	Il punteggio DPC potrebbe essere diminuito di 1, ad esempio quando la natura dei dati può portare a supposizioni su informazioni sensibili.	3

A2 Descrizione dei fattori contestuali da considerare nel punteggio DPC

Fattori crescenti:

- ✓ **Il volume dei dati violati (per lo stesso individuo)**: questo fattore può aumentare il punteggio DPC di base, a causa dell'aumento della quantità di informazioni violate (cioè agendo come fattore aggravante). Il volume deve essere considerato sia in termini di tempo (ad esempio, lo stesso tipo di dati per un certo periodo di tempo) che di contenuto (dati complementari dello stesso tipo). Ad esempio, in caso di violazione dei dati sul traffico di un ISP, il punteggio DPC sarà più alto (per lo stesso individuo) se i dati coprono un periodo di un anno rispetto a quelli limitati a una settimana (tempo). Per fare un altro esempio, in caso di violazione di una banca, il punteggio DPC dell'intero file di un individuo sarebbe più alto di quello di un singolo documento dello stesso file (contenuto).

- ✓ **Caratteristiche particolari del titolare del trattamento**: questo fattore riguarda il campo operativo e le attività del titolare del trattamento, che potrebbero aumentare il punteggio DPC di base dei dati, rivelando informazioni aggiuntive per un determinato set di dati. Ad esempio, il punteggio DPC di un elenco di clienti sarà più alto se proviene da una farmacia online piuttosto che da una cartoleria.

- ✓ **Caratteristiche speciali degli individui**: il punteggio DPC di base di un determinato set di dati potrebbe anche essere aumentato nel caso in cui gli individui appartengano a un gruppo sociale con esigenze particolari (ad esempio, minori, individui di un gruppo particolare con caratteristiche speciali). Ad esempio, il punteggio DPC di un elenco di numeri di telefono aumenterebbe se si trattasse di membri noti del Parlamento nazionale.

Fattori decrescenti:

- ✓ **Invalidità/accuratezza dei dati**: il punteggio DPC di base di un determinato insieme di dati può essere ridotto se il responsabile del trattamento è a conoscenza dell'invalidità o dell'inaccuratezza dei dati (ad esempio, a causa della loro età o del loro contenuto) e, quindi, la loro importanza è ridotta. Il responsabile del trattamento deve essere certo di questa circostanza per includerla nella valutazione. Ad esempio, l'elenco di un servizio postale di indirizzi in cui non è stato possibile consegnare le lettere sarebbe considerato inesatto (cioè, molto probabilmente le persone si sono trasferite a un altro indirizzo).

- ✓ **Disponibilità pubblica**: il punteggio DPC di base di un set di dati può essere ridotto anche nel caso in cui i dati violati fossero già disponibili al pubblico prima della violazione o potessero essere facilmente raccolti e/o consultati attraverso fonti disponibili al pubblico.

- ✓ **Natura dei dati**: un altro fattore di diminuzione potrebbe essere, in alcuni casi, la natura stessa di un particolare set di dati che, nonostante il punteggio DPC iniziale, è di minore importanza, in termini di informazioni che può rivelare sull'individuo. È il caso, ad esempio, di un certificato medico che si limita a certificare che l'individuo è in buono stato di salute senza rivelare altre informazioni. In questo caso, anche se il punteggio di base sarebbe 4, in quanto i dati sanitari sono dati sensibili, il punteggio finale del set di dati specifici sarebbe 1, in quanto non può di per sé influire sulla vita personale dell'individuo. Questo fattore, tuttavia, dovrebbe essere considerato con grande attenzione e con una chiara spiegazione del motivo per cui un particolare trattamento di dati è per natura inferiore al suo punteggio DPC di base.

A3 Esempi di punteggio/rettifica del DPC per categoria di dati

Dati semplici

Esempio 1: Elenco di nomi e numeri di telefono

- **Caso 1: l'elenco è quello dei clienti di un supermercato/ristorante. Punteggio = 1 (nessuna alterazione dovuta a fattori contestuali)**
- Caso 2: l'elenco proviene da un'azienda che vende auto/case di lusso.
  Punteggio= 2 (per le caratteristiche del controllore che portano a supposizioni sullo status finanziario/sociale)
- Caso 3: l'elenco proviene da una farmacia elettronica specializzata nella vendita di prodotti per pazienti affetti da diabete.
  Punteggio= 3 (per caratteristiche del controllore che portano a supposizioni sullo stato di salute dell'individuo)
- Caso 4: la lista include i nomi di persone che lavorano sotto copertura per la polizia segreta. Punteggio= 4 (per le caratteristiche degli individui che potrebbero essere critiche per la loro sicurezza personale)

Esempio 2: un database di CV professionali

- **Caso 1: i dati provengono da un sito di carriera online in cui l'accesso ai CV è disponibile per gli utenti registrati. Punteggio= 1 (nessuna alterazione dovuta a fattori contestuali)**
- Caso 2: i dati provengono da un'organizzazione che aiuta i disoccupati a trovare lavoro.
  Punteggio= 2 (in base alle caratteristiche del controllore che portano a supposizioni sullo stato finanziario/sociale)
- Caso 3: i dati provengono da un'istituzione che sostiene i diritti degli omosessuali.
  Punteggio= 3 (per le caratteristiche del controllore che portano a formulare ipotesi sulla vita sessuale dell'individuo).
- Caso 4: i dati provengono da un'organizzazione che aiuta i tossicodipendenti in fase di recupero a trovare lavoro.
  Punteggio= 4 (per le caratteristiche degli individui che potrebbero causare loro gravi danni).

Esempio 3: Elenco di nomi e indirizzi postali

- **Caso 1: l'elenco è quello dei clienti di un negozio di fiori. Punteggio = 1 (nessuna alterazione dovuta a fattori contestuali)**
- Caso 2: l'elenco proviene da una banca d'investimento.
  Punteggio= 2 (per le caratteristiche del controllore che portano a supposizioni sullo status finanziario/sociale)
- Caso 3: l'elenco è costituito dagli indirizzi di consegna di un negozio di libri per adulti.
  Punteggio= 3 (per caratteristiche del controllore che portano a supposizioni sulle preferenze sessuali dell'individuo)

- Caso 4: l'elenco riguarda persone che sono state accusate di abusi su minori.

  Punteggio= 4 (per le caratteristiche delle persone che potrebbero causare loro gravi danni)

Dati comportamentali

Esempio 1: cronologia delle chiamate telefoniche (dati di traffico - nessun contenuto)

- Caso 1: i dati provengono dall'helpdesk di un ISP e comprendono le chiamate in entrata degli abbonati all'helpdesk per problemi tecnici.

  Punteggio= 1 (per la natura del set di dati).

- **Caso 2: i dati provengono da un ISP e comprendono la cronologia delle chiamate degli abbonati dell'ultima settimana.**

  Punteggio = 2 (nessuna alterazione dovuta a fattori contestuali).

- Caso 3: i dati provengono da un ISP e includono la cronologia delle chiamate degli abbonati dell'ultimo anno.

  Punteggio = 3 (è possibile creare un profilo dettagliato dell'individuo).

- Caso 4: i dati provengono da un centro di sostegno psicologico per persone affette da una grave malattia e comprendono le chiamate in entrata.

  Punteggio= 4 (per caratteristiche del controllore che rivela lo stato di salute).

Esempio 2: Dati in una fidelity card

- Caso 1: la carta proviene da un supermercato e include solo il numero di punti guadagnati con gli acquisti.

  Punteggio= 1 (per la natura del set di dati).

- **Caso 2: la carta proviene da un supermercato e include informazioni sullo storico degli acquisti dell' ultimo mese.**

  Punteggio= 2 (nessuna alterazione dovuta a fattori contestuali).

- Caso 3: i dati provengono da una carta di trasporto e includono informazioni sulla posizione/gli spostamenti nell'ultimo anno.

  Punteggio= 3 (è possibile creare un profilo dettagliato dell'individuo).

- Caso 4: la carta proviene da una farmacia e contiene informazioni sugli acquisti recenti di prodotti medici.

  Punteggio= 4 (per la natura del set di dati che rivela dati sensibili).

Esempio 3: dati provenienti da un social network

- Caso 1: i dati sono pubblicamente disponibili su Internet (ad es. foto che l'utente ha pubblicato online).

  Punteggio= 1 (per disponibilità pubblica).

- **Caso 2: i dati includono informazioni sulle preferenze e sulla vita quotidiana dell'utente nell'ultimo mese, che l'utente ha condiviso con i suoi amici (ad esempio, informazioni pubblicate sulla bacheca dell'utente).**

  Punteggio= 2 (nessuna alterazione dovuta a fattori contestuali).

- Caso 3: i dati includono informazioni sulle preferenze dell'utente e sulla sua vita quotidiana dell'ultimo anno che l'utente ha condiviso con i suoi amici (ad esempio, informazioni pubblicate sulla bacheca dell'utente).

Punteggio= 3 (è possibile creare un profilo dettagliato dell'individuo).

- Caso 4: i dati includono comunicazioni personali (ad es. messaggi personali) che possono rivelare informazioni sulla vita sessuale o sullo stato di salute dell'utente.

  Punteggio= 4 (porta alla creazione di un profilo dettagliato relativo a dati sensibili).

Dati finanziari

Esempio 1: estratti conto bancari

- Caso 1: i dati provengono da una banca e includono solo una lettera, attraverso la quale l'individuo è identificato come cliente senza fornire alcuna informazione sulle relazioni specifiche tra il cliente e la banca (ad esempio, solo il suo nome e indirizzo, ma nessun numero di conto o informazioni sulle transazioni).

  Punteggio= 1 (per la natura del set di dati).

- Caso 2: i dati provengono da una banca e includono solo la cronologia delle transazioni di un giorno senza ulteriori dettagli (ad esempio, numero di conto, nome e transazione).

  Punteggio = 2 (per la natura dei dati, informazioni che possono portare a informazioni limitate sul comportamento finanziario).

- **Caso 3: i dati provengono da una banca e riguardano i saldi dei conti dei clienti dell'ultimo mese.**

  Punteggio= 3 (nessuna alterazione dovuta a fattori contestuali).

- Caso 4: i dati provengono da una banca e includono i saldi dei conti dei clienti dell'ultimo anno, mostrando tutte le transazioni e i relativi dettagli.

  Punteggio= 4 (per il volume e la natura dei dati che portano alla profilazione).

Esempio 2: dichiarazione dei redditi

- Caso 1: i dati contengono una dichiarazione che conferma che l'individuo ha presentato la sua dichiarazione di reddito.

  Punteggio= 1 (per la natura del set di dati).

- Caso 2: i dati contengono la percentuale di tasse che l'individuo deve pagare. Punteggio= 2 (per la natura dei dati, informazioni che possono portare a informazioni limitate sullo stato finanziario).

- **Caso 3: i dati contengono tutti i campi della dichiarazione dei redditi di un anno dell'individuo. Punteggio = 3 (nessuna alterazione dovuta a fattori contestuali).**

- Caso 4: i dati contengono tutti i campi della dichiarazione dei redditi dell'individuo per gli ultimi 10 anni.

  Punteggio= 4 (per il volume e la natura dei dati che portano a una profilazione dettagliata).

Esempio 3: informazioni sulla carta di credito

- Caso 1: i dati provengono da una banca e contengono i dati della carta di credito di un individuo, ma questi dati risalgono a più di dieci anni fa e quindi le carte non sono valide.

  Punteggio= 1 (per età del set di dati).

- Caso 2: i dati provengono da un negozio online e contengono alcune informazioni sulle carte di credito delle persone, ma non l'insieme di dettagli necessari per eseguire transazioni finanziarie.

  Punteggio= 2 (per la natura dei dati, informazioni che possono portare a informazioni limitate sullo stato finanziario).

- **Caso 3: i dati provengono da una banca e contengono alcune informazioni sulle carte di credito degli individui, ma non l'insieme di dettagli necessari per effettuare transazioni finanziarie. Tuttavia, contengono informazioni su alcuni acquisti delle persone per un periodo di un anno.**

  Punteggio= 3 (nessuna alterazione dovuta a fattori contestuali).

- Caso 4: i dati provengono da un negozio online e contengono tutti i dettagli della carta di credito che possono essere utilizzati per le transazioni finanziarie.

  Punteggio= 4 (il set di dati potrebbe essere utilizzato per frodi).

Dati sensibili

Esempio 1: Dati sulle analisi del sangue

- Caso 1: i dati provengono da un laboratorio e includono solo l'indicazione che gli individui hanno eseguito analisi del sangue generali.

  Punteggio= 1 (per la natura dei dati).

- Caso 2: i dati provengono da un laboratorio di un pronto soccorso di un ospedale e includono solo informazioni sul fatto che le persone hanno eseguito analisi del sangue (senza ulteriori dettagli).

  Punteggio= 2 (per la natura dei dati che portano a ipotesi generali).

- Caso 3: i dati provengono da un laboratorio e includono l'indicazione che gli individui hanno eseguito test per una certa malattia, senza indicazione dei risultati. Punteggio = 3 (per la natura dei dati che portano a supposizioni che potrebbero causare danni all'individuo).

- **Caso 4: i dati provengono da un laboratorio e includono i risultati dei test. Punteggio = 4 (nessuna**

  alterazione dovuta a fattori contestuali).

Esempio 2: Dati sull'affiliazione politica

- Caso 1: i dati provengono da un importante partito politico e includono i nomi di membri di spicco che ricoprono posizioni pubbliche e la loro affiliazione al partito è pubblicamente nota.

  Punteggio= 1 (per la natura dei dati).

- Caso 2: i dati provengono da una società che organizza eventi e includono i nomi di persone che hanno partecipato a un evento di beneficenza sponsorizzato da uno specifico partito politico.

  Punteggio= 2 (per la natura dei dati che portano a ipotesi generali).

- Caso 3: i dati provengono da un partito politico e includono i nomi di persone che hanno partecipato a una specifica conferenza organizzata dal partito.

  Punteggio = 3 (per la natura dei dati che portano a supposizioni che potrebbero causare danni all'individuo).

- **Caso 4: i dati provengono da un forum chiuso su Internet e includono le opinioni politiche espresse dai membri del forum.**

  Punteggio= 4 (nessuna alterazione dovuta a fattori contestuali).

Esempio 3: dati sulla vita sessuale

- Caso 1: i dati provengono da un forum di discussione online sulle relazioni e includono solo il nome degli utenti registrati senza ulteriori informazioni.

  Punteggio= 1 (per la natura dei dati).

- Caso 2: i dati provengono da un sito di incontri e includono solo il nome dei clienti senza altre informazioni.

  Punteggio= 2 (per la natura dei dati che porta a ipotesi generali).

- Caso 3: i dati provengono da un sito di incontri specializzato, ma non esclusivo, in incontri eterosessuali o gay e includono il nome dei clienti.

- Punteggio= 3 (per la natura dei dati che porta a fare ipotesi su informazioni sensibili).

- **Caso 4: i dati provengono da un sito di incontri e includono l'orientamento sessuale dichiarato dei clienti.**

  Punteggio= 4 (nessuna alterazione dovuta a fattori contestuali).

Credenziali

Esempio: Nome utente e password degli utenti registrati in un servizio online.

- Caso 1: le credenziali sono utilizzate per accedere agli account degli utenti di un negozio di musica elettronica. Punteggio =

  1 / Dati semplici (nessuna alterazione dovuta a fattori contestuali)

- Caso 2.1: le credenziali sono utilizzate per accedere agli account degli utenti nel sito web di un supermercato, comprese le informazioni sulle liste della spesa precedenti.

  Punteggio= 2 / Dati comportamentali (nessuna alterazione dovuta a fattori contestuali)

- Caso 2.2: le credenziali sono utilizzate per accedere agli account degli utenti di un sito di social media. Punteggio = 3

  / Dati comportamentali con profilazione dettagliata

- Caso 3.1: le credenziali possono essere utilizzate per l'accesso all'account dell'utente nel sistema fiscale nazionale, fornendo informazioni sul reddito dell'utente.

  Punteggio= 3 / Dati finanziari (nessuna alterazione dovuta a fattori contestuali)

- Caso 3.2: le credenziali possono essere utilizzate per l'online banking con la possibilità di effettuare transazioni finanziarie (es. trasferimento di denaro).

  Punteggio= 4 / Dati finanziari con informazioni finanziarie complete e possibilità di frode.

- Caso 4: le credenziali vengono utilizzate per l'accesso agli account degli utenti di una comunità online relativa alle preferenze sessuali.

  Punteggio= 4 / Dati sensibili (nessuna alterazione dovuta a fattori contestuali).

Allegato 2 - Punteggio della facilità di identificazione (EI)

Questo allegato presenta esempi di punteggio EI per identificatori comuni.

L'identificazione può essere diretta o indiretta e viene effettuata con l'uso di determinati identificatori, tenendo conto anche del contesto generale del trattamento dei dati personali. I prossimi esempi mostrano un elenco (non esaustivo) di identificatori comuni e diversi casi del loro possibile utilizzo per la determinazione dell'IE.

Va notato che in molti casi la violazione includerà una combinazione di diversi identificatori, il che aumenta automaticamente la facilità di identificazione. Si tratta di un elemento molto importante che deve essere preso in considerazione dal responsabile del trattamento e che si riflette negli esempi che seguono.

Nome e cognome (nome, cognome)

È considerato l'identificatore diretto più comune, ma il punteggio dell'IE può variare a seconda dei casi, poiché il nome completo non sempre individua di per sé in modo univoco l'individuo. Ad esempio, quando l'identificazione viene effettuata utilizzando solo il nome completo dell'individuo:

- EI = 0,25 (trascurabile) in tutta la popolazione di un paese in cui molte persone condividono lo stesso nome completo
- EI= 0,5 (limitato) in un Paese in cui poche persone condividono lo stesso nome completo.
- EI= 0,75 (Significativo) in tutta la popolazione di una piccola città in cui poche o nessuna persona condivide lo stesso nome completo.
- EI=1 (massimo) in tutta la popolazione di un paese che utilizza anche la data di nascita e l'indirizzo e-mail.

Carta d'identità/passaporto/numero di previdenza sociale

Sono tutti considerati identificatori univoci e possono essere utilizzati per individuare un individuo, purché sia possibile collegarli a un database di riferimento (ad esempio, collegando una carta d'identità a una determinata persona). Ad esempio, quando l'identificazione viene effettuata utilizzando solo uno di questi numeri:

- EI=0,25 (trascurabile) quando non vengono fornite altre informazioni sull'individuo o non è possibile reperire ulteriori informazioni a meno che non si ottenga l'accesso al database di riferimento
- EI=0,75 (Significativo) quando l'identificatore rivela informazioni aggiuntive sull'individuo (ad esempio, numero di previdenza sociale che rivela la data di nascita) ed è collegato ad altri dati (ad esempio, indirizzo postale o e-mail).
- EI=1 (massimo) quando sono disponibili anche informazioni dal database di riferimento (ad es. carta d'identità e nome e cognome e/o foto).

Numero di telefono/indirizzo di casa

Sono entrambi identificatori indiretti, che possono essere utilizzati per comunicare con l' individuo o per accedervi. Quando l'identificazione si basa solo su uno di questi due identificatori:

- EI=0,25 (Trascurabile) in tutta la popolazione di un paese quando il numero/indirizzo non è registrato in un registro pubblico.
- EI=0,5 (Limitato) su tutta la popolazione di una piccola città e il numero/indirizzo non è registrato in un registro pubblico (identificazione possibile attraverso la comunicazione).
- EI=1 (Massimo) su tutta la popolazione di un paese e il numero/indirizzo è incluso in un registro disponibile al pubblico.

Indirizzo e-mail

È un identificatore indiretto, che può essere utilizzato per comunicare con l'individuo e in alcuni casi può includere informazioni sul suo nome (nome e/o cognome). Quando l'identificazione è basata sull'e-mail:

- EI=0,25 (trascurabile) quando l'indirizzo e-mail non rivela altre informazioni di identificazione (ad esempio, il nome) e non viene utilizzato come indirizzo principale dell'individuo in siti Internet, forum o social network.
- EI=0,75 (Significativo) quando l'indirizzo e-mail non rivela altre informazioni identificative (ad esempio il nome) ma viene utilizzato come indirizzo principale dell'individuo in siti Internet, forum o social network (ricercabili sul web).
- EI=1 (massimo) quando l'indirizzo e-mail rivela il nome dell'individuo e viene utilizzato come indirizzo principale in siti internet, forum o social network (ricercabili sul web).

Immagine

Può essere un identificatore diretto o indiretto, a seconda dei casi. Ad esempio, quando l'identificazione si basa solo su un'immagine:

- EI=0,25 (Trascurabile) quando l'immagine è poco chiara o vaga (ad esempio, filmati di telecamere a circuito chiuso da una lunga distanza).
- EI=05 (Limitato) quando l'immagine è poco chiara o vaga ma include informazioni aggiuntive (ad esempio, dintorni che mostrano un luogo specifico) che potrebbero portare all'identificazione dell'individuo.
- EI=0,75 (Significativo) quando l'immagine è chiara ma non contiene altre informazioni per l'identificazione.
- EI=1 (massimo) quando l'immagine è chiara e collegata ad alcune informazioni aggiuntive (ad esempio, informazioni sull'appartenenza a un gruppo specifico, indirizzo di casa, ecc.)

Codifica/Alias/Iniziali

La codifica si riferisce all'assegnazione di un numero identificativo univoco a ciascun individuo, ad esempio nel contesto di un database specifico. L'uso di pseudonimi è una forma di pseudonimizzazione, nel senso che un identificatore specifico (di solito il nome completo dell'individuo) viene sostituito da un alias (pseudonimo). Le iniziali sono un tipo di alias che viene estratto dal nome completo dell'individuo. Come nel caso degli identificatori univoci, i codici e gli pseudonimi possono essere utilizzati per identificare l'individuo, purché sia possibile collegarli a un database di riferimento (ad esempio, collegando il codice/alias al nome completo di una determinata persona) Quando l'identificazione si basa sulla codifica o sull'uso di pseudonimi:

- EI=0,25 (trascurabile) quando il codice/alias non rivela e non può essere collegato ad altri dati personali dell'individuo a meno che non si ottenga l'accesso alla banca dati di riferimento.
- EI=0,75 (significativo) quando l'alias rivela alcuni dati sull'individuo (ad esempio, il nome) ed è collegato ad altri dati personali (ad esempio, l'indirizzo e-mail dell'individuo).
- EI=1 (massimo) quando l'alias rivela il nome completo dell'individuo o sono disponibili anche i dati del database di riferimento.

Allegato 3 - Esempi di circostanze della violazione (CB) con punteggio

A1 Perdita di riservatezza

0 - Esempi di dati esposti a rischi di riservatezza senza prove di un trattamento illecito.

- ✓ Un file cartaceo o un computer portatile viene smarrito durante il trasporto.
- ✓ L'apparecchiatura è stata smaltita senza distruggere i dati personali.

+0,25 - Esempi di dati smaltiti a più destinatari noti:

- ✓ Un'e-mail con dati personali è stata erroneamente inviata a più destinatari noti.
- ✓ Alcuni clienti hanno potuto accedere agli account di altri clienti in un servizio online.

+0,5 - Esempi di dati ceduti a un numero imprecisato di destinatari:

- ✓ I dati sono pubblicati su una bacheca internet.
- ✓ I dati vengono caricati su un sito P2P.
- ✓ Un dipendente vende un CD ROM con i dati dei clienti.
- ✓ Un sito Web configurato in modo errato rende pubblicamente accessibili su Internet i dati degli utenti interni.

A2 Perdita di integrità

0 - Esempi di dati alterati senza che sia stato identificato un uso scorretto o illegale:

- ✓ Le registrazioni di un database con dati personali sono state aggiornate in modo errato, ma l'originale è stato ottenuto prima di qualsiasi utilizzo dei dati alterati.

+0,25 - Esempi di dati alterati ed eventualmente utilizzati in modo scorretto o illegale, ma con possibilità di recupero:

- ✓ Un record necessario per la fornitura di un servizio sociale online è stato modificato e l'individuo deve richiedere il servizio in modo offline.
- ✓ Un record importante per l'accuratezza del file di un individuo in un servizio medico online è stato modificato.

+0,5 - Esempi di dati alterati ed eventualmente utilizzati in modo scorretto o illegale senza possibilità di recupero:

- ✓ Gli esempi precedenti+ l'originale non può essere recuperato.

A3 Perdita di disponibilità

0 - Esempi di dati recuperabili senza alcuna difficoltà:

- ✓ Una copia di un file viene persa ma altre copie sono disponibili.
- ✓ Un database è danneggiato ma può essere facilmente ricostruito da altri database.

+0,25 - Esempi di indisponibilità temporale:

- ✓ Un database è danneggiato ma può essere ricostruito da altri database, anche se è necessaria una certa elaborazione.
- ✓ Un file è perso, ma le informazioni possono essere fornite nuovamente dall'individuo.

+0,5 - Esempi di indisponibilità completa (i dati non possono essere recuperati dal controllore o dalle persone):

- ✓ Un file è perso/database danneggiato, non c'è un backup di queste informazioni e non possono essere fornite dall'individuo.

A4 Intenzione dolosa

+0,5 - La violazione è dovuta a un'azione intenzionale, ad esempio per causare problemi al titolare del trattamento (ad esempio, dimostrare la perdita di sicurezza) e/o per danneggiare le persone.

- ✓ Un dipendente di un'azienda condivide intenzionalmente i dati privati dei clienti su un sito pubblico di social media.
- ✓ Un dipendente di un'azienda vende i dati privati dei clienti a un'altra azienda.
- ✓ Un membro di un social network invia intenzionalmente informazioni su altri membri ai loro familiari per danneggiarli.

TP-04-13-118-IT-N

ENISA
Agenzia dell'Unione Europea per la sicurezza delle reti e dell'informazione Parco scientifico e tecnologico di Creta (ITE)
Vassilika Vouton, 700 13, Heraklion, Grecia

Ufficio di Atene
1 Vass. Sofias & Meg. Alexandrou Marousi
151 24, Atene, Grecia

PO Box 1309, 710 01 Heraklion, Grecia
Tel: +30 28 14 40 9710
info@enisa.europa.eu www.enisa.europa.eu

Registro dei data breach
(art. 30 Reg. EU 679/2016)

Titolare del trattamento	
	Comune di Valdastico – Istituzione "Cav. Paolo Sartori"
Forma giuridica	Istituzione comunale ai sensi dell'art. 114 del D.Lgs. 267/2000. La personalità giuridica è in capo al Comune di Valdastico.
Indirizzo della sede	Via Cav. Paolo Sartori n. 20 – 36040 Valdastico (VI)
Dati di contatto del Titolare	Telefono: 0445-745029 i. 3 E-mail: info@casanostravaldastico.it PEC: casanostravaldastico@pecveneto.it
Codice fiscale e Partita IVA	C.F. 84001010242 – P. IVA 01513240240
Responsabile della protezione dei dati (RPD-DPO)	
	In4data di Finco Matteo, nella persona di Finco Eric
Dati di contatto del RPD-DPO	E-mail: info@in4data.it PEC: legal@pec.in4data.it
Partita IVA	P. IVA 04477810248

Rappresentante

Non presente

REGISTRO DATA BREACH

CODICE	SEGNALAZIONE				VIOLAZIONE					INTERESSATI e DATI				CONSEGUENZE		ATTENUAZIONE		PREVENZIONE FUTURA		NOTIFICA AL GARANTE					COMUNICAZIONE AGLI INTERESSATI				SEGNALAZIONE AD AUTORITÀ GIUDIZIARIA O DI POLIZIA	NOTE	ESTENSORE
codice evento	data e ora della segnalazione (e aggiornamenti)	modalità con la quale il titolare è venuto a conoscenza della violazione	unità organizzativa coinvolta	destinatari della segnalazione	data e ora della violazione (se conosciuta)	causa della violazione	sistemi/apparati/reti/banche dati oggetto di data breach	natura della violazione dei dati personali	altri elementi utili alla descrizione della violazione	categorie di interessati	numero approssimativo di interessati	categorie dei dati personali	numero approssimativo di registrazioni dei dati personali	conseguenze della violazione dei dati personali	gravità	misure adottate per per attenuare i possibili effetti negativi	misure di cui si propone l'adozione per attenuare i possibili effetti negativi	misure adottate per prevenire simili violazioni in futuro	misure di cui si propone l'adozione per prevenire simili violazioni in futuro	rischio per i diritti e le libertà delle persone fisiche	invio di notificazione alla DPA	ragioni dell'invio di notificazione parziale	ragioni del ritardo della notificazione alla DPA	ragioni di omessa notifica alla DPA	indicare se ricorre rischio elevato per i diritti e le libertà delle persone fisiche	comunicazione agli interessati	modalità della comunicazione agli interessati	ragioni della omessa comunicazione agli interessati	indicare se è stata effettuata una segnalazione ad altre autorità	note	identificativo estensore