AREU
Sistema Socio Sanitario
Regione Lombardia

DELIBERA DEL DIRETTORE GENERALE

302 / 2023 del 24/10/2023

***Oggetto*: APPROVAZIONE DELLA POLITICA GENERALE DI PROTEZIONE DEI DATI PERSONALI**

AREU Agenzia Regionale Emergenza Urgenza
Via Alfredo Campanini, 6 - 20124 Milano | C.F. e P. IVA 11513540960
Tel 02 67129001 | Fax 02 67129002 | Mail protocollo@pec.areu.lombardia.it
www.areu.lombardia.it

OGGETTO: APPROVAZIONE DELLA POLITICA GENERALE DI PROTEZIONE DEI DATI PERSONALI

vista la seguente proposta di deliberazione n. 554/2023, avanzata dal Direttore della Struttura Complessa Affari Generali e Legali

IL DIRETTORE GENERALE

PREMESSO che AREU è un Ente del SSR disciplinato dall'art. 16 LR 30/12/2009 n. 33 e ss.mm.ii., attivato dalla DGR n. 2701/2019 e dalla DGR n. 4078/2020 con il compito di implementare e rendere omogeneo nel territorio regionale il soccorso sanitario di emergenza urgenza extraospedaliera, nonché di coordinare le attività trasfusionali ed il trasporto di équipe di trapianto, persone ed organi, unitamente alla gestione del servizio di "Numero Unico Emergenza 112" e del "Numero Europeo Armonizzato" (NEA) 116117, per l'accesso ai servizi di cure mediche non urgenti e altri servizi sanitari, la cui attivazione concorre alla gestione della domanda assistenziale a bassa intensità/priorità;

DATO ATTO che:

- il Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (General Data Protection Regulation, o GDPR), applicabile in tutti gli Stati membri dell'Unione Europea a partire dal 25 maggio 2018, nell'affrontare il tema della tutela dei dati personali attraverso un approccio basato principalmente sulla valutazione dei rischi, sui diritti e le libertà degli interessati, attribuisce ai Titolari del trattamento (nel caso, a questa Agenzia) il potere di adottare le misure che ritiene più idonee ed opportune per garantire la protezione dati personali;
- il "sistema privacy" delineato dal GDPR implica la necessità di infondere nell'organizzazione aziendale la piena consapevolezza dei rischi inerenti ai trattamenti, nonché l'affermazione di una cultura della protezione dei dati quale parte integrante dell'intero asset organizzativo, con particolare attenzione alle categorie particolari di dati, tra i quali quelli relativi alla salute;
- il nuovo approccio comporta il coinvolgimento di tutti i soggetti chiamati a trattare i dati personali all'interno dell'organizzazione aziendale, con assunzione delle relative responsabilità;

RICHIAMATA la principale novità introdotta dal GDPR, ovvero il principio di "responsabilizzazione" (c.d. accountability) consistente in un approccio metodologico basato sulla preliminare valutazione dei rischi potenzialmente lesivi dei diritti e delle libertà degli interessati, sulla base del quale si attribuisce ai Titolari del trattamento il compito di assicurare ed essere in grado di comprovare il rispetto dei principi applicabili al trattamento dei dati personali e di adottare quelle misure tecniche e organizzative che vengano valutate a ciò più idonee ed opportune;

RITENUTO che la piena realizzazione del suddetto principio di accountability e del nuovo approccio che ne deriva all'interno dell'organizzazione aziendale, passino anche attraverso la emanazione di una Politica generale di protezione dei dati personali che

fornisca una linea guida per l'applicazione della materia nei vari ambiti in cui quotidianamente si esplica l'attività istituzionale dell'Agenzia;

RITENUTO altresì che una Politica generale di protezione dei dati personali possa costituire uno strumento di ausilio affinché il trattamento dei dati personali da parte degli operatori dell'Agenzia avvenga nel rispetto dei diritti, delle libertà fondamentali, della dignità di tutti gli interessati, con particolare riferimento alla loro riservatezza;

VISTA la Delibera del Direttore Generale n. 94 del 11.04.2023 con la quale è stato costituito all'interno dell'Agenzia un gruppo di lavoro trasversale e multidisciplinare di supporto dell'Ente per l'applicazione del GDPR, denominato "Gruppo Privacy", che costituisce l'interfaccia del DPO e il punto di riferimento per l'elaborazione ed approvazione di tutte le procedure necessarie alla corretta implementazione del sistema di gestione aziendale della protezione dei dati;

DATO ATTO che è stato demandato alla SC Affari generali e Legali, il compito di predisporre tale Politica generale di protezione dei dati personali che è stata vagliata dal Gruppo Privacy nella seduta del 05.10.2023;

RITENUTO pertanto di adottare il documento relativo alla "Politica generale di protezione dei dati personali", allegata quale parte integrante e sostanziale del presente provvedimento;

PRESO ATTO che il Proponente del procedimento attesta la completezza, la regolarità tecnica e la legittimità del presente provvedimento;

ACQUISITI i pareri favorevoli del Direttore Amministrativo F.F. e del Direttore Sanitario, resi per quanto di specifica competenza ai sensi dell'art. 3 del D.Lgs. n. 502/1992 e s.m.i.;

DELIBERA

Per tutti i motivi in premessa indicati e integralmente richiamati:

1. di approvare il testo del documento "Politica generale di protezione dei dati personali", allegato quale parte integrante e sostanziale del presente provvedimento;
2. di dare atto che, ai sensi della L. n. 241/1990, responsabile del presente procedimento è la Dott.ssa Domenica De Giorgio, Dirigente S.C. Affari Generali e Legali;
3. di dare atto che dal presente provvedimento non derivano oneri a carico del bilancio aziendale;
4. di disporre che vengano rispettate tutte le prescrizioni inerenti alla pubblicazione sul portale web aziendale di tutte le informazioni e i documenti richiesti e necessari ai sensi del D.Lgs. n. 33/2013 e s.m.i., c.d. Amministrazione Trasparente;
5. di disporre la pubblicazione del presente provvedimento all'Albo Pretorio on line dell'Agenzia, dando atto che lo stesso è immediatamente esecutivo (ex art. 32 comma 5 L. n. 69/2009 s.m.i. e art. 17 comma 6 L.R. n. 33/2009).

La presente delibera è sottoscritta digitalmente, ai sensi dell'art. 21 D.Lgs. n. 82/2005 e s.m.i., da:

Per il Direttore Amministrativo Andrea Albonico come da delega acquisita agli atti dell'Agenzia Marco Michele Gelmetti

Il Direttore Sanitario Giuseppe Maria Sechi

Il Direttore Generale Alberto Zoli

POLITICA GENERALE DI PROTEZIONE DEI DATI PERSONALI

AREU Agenzia Regionale Emergenza Urgenza
Via Alfredo Campanini, 6 - 20124 Milano | C.F. e P. IVA 11513540960
Tel 02 67129001 | Fax 02 67129002 | Mail protocollo@pec.areu.lombardia.it
www.areu.lombardia.it

Sommario

Premesse

L'Agenzia Regionale Emergenza Urgenza (di seguito anche AREU) con il presente documento ha inteso adottare una Politica Generale di Protezione dei Dati Personali, nel rispetto della normativa specifica, al fine di disciplinare il sistema di gestione aziendale e assicurare la piena liceità e correttezza nei trattamenti eseguiti.

Nel documento sono brevemente esposti i principi che regolano le attività di trattamento di dati personali eseguite dall'Agenzia, le figure coinvolte nel sistema di gestione aziendale, con le rispettive competenze e responsabilità e le misure organizzative adottate per garantire un corretto governo dei trattamenti eseguiti.

Riferimenti normativi e documentali e ambito di applicazione

La Politica Generale di Protezione Dati Personali di AREU è stata redatta in attuazione delle seguenti disposizioni:

- Reg. UE 2016/679 (Regolamento Generale Protezione Dati)
- D.Lgs. 196/2003 (Codice Protezione Dati Personali)
- D.Lgs. 101/2018 (Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016)

Il presente documento trova applicazione nei confronti di tutto il personale dell'Agenzia, indipendentemente dalla tipologia del rapporto e, delle Terze Parti che, nell'ambito delle proprie mansioni o delle attività professionali svolte per conto dell'Agenzia, compiano operazioni di trattamento su dati personali sotto la responsabilità delle stesse.

Definizioni

Le seguenti definizioni sono utili a comprendere i termini utilizzati nella presente Politica Generale per la Protezione dei Dati Personali:

Soggetti interessati: Il "soggetto interessato" è definito nell'articolo 4(1) del Reg. UE 2016/679 come la persona fisica identificata o identificabile a cui si riferiscono i dati personali.

Dati personali: Secondo l'articolo 4(1) del Reg. UE 2016/679 (GDPR), i "dati personali" sono definiti come qualsiasi informazione riguardante una persona fisica identificata o identificabile

('interessato'); un individuo identificabile è una persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento a un identificativo come un nome, un numero di identificazione, dati di localizzazione, un identificatore online o a uno o più fattori specifici dell'identità fisica, fisiologica, genetica, mentale, economica, culturale o sociale di tale individuo". Gli esempi possono includere il nome, l'indirizzo e-mail, il numero di telefono, l'indirizzo IP, ecc.

Categorie particolari di dati personali (dati sensibili): Il Reg. UE 2016/679, articolo 9(1), definisce i "dati sensibili" o "categorie particolari di dati personali" come dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, i dati genetici, i dati biometrici per l'identificazione univoca di una persona fisica, i dati relativi allo stato di salute o alla vita sessuale o all'orientamento sessuale di una persona. Gli esempi possono includere la religione di una persona, il suo orientamento sessuale, le informazioni genetiche, ecc.

Dati relativi a condanne penali e reati: Il Reg. UE 2016/679 non definisce all'articolo 10 come tutte le informazioni riguardanti le condanne penali, le accuse, i certificati casellari, ecc. Questo tipo di dati può essere trattato solo sotto il controllo dell'autorità pubblica o quando la legge dell'UE o degli Stati membri lo prevede.

Trattamento di dati personali: 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.

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

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

Soggetti autorizzati al trattamento: la persona fisica sottoposta alla direzione del Titolare del trattamento, come i dipendenti, che ha il permesso di trattare dati personali nel corso delle sue attività lavorative ed è specificatamente istruito in merito.

Destinatari: 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 altri titolari, responsabili, persone autorizzate o soggetti interessati.

Violazione di 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.

Valutazione d'impatto: un processo documentato che ha lo scopo di identificare, valutare e gestire i rischi per i soggetti interessati derivanti dal trattamento dei loro dati personali, nonché valutare la conformità del trattamento stesso.

Principi che regolano il trattamento dei dati

Nello svolgimento di ogni attività di trattamento dei dati, AREU opera in conformità ai principi sanciti dalla normativa nazionale e comunitaria.

In particolare, i dati devono essere:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità correttezza e trasparenza" - Articolo 5, par. 1, lett. a) Reg. UE/679/2016);
- raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non siano incompatibili con tali finalità ("limitazione della finalità" - Articolo 5, paragrafo 1, lett. b), Reg. UE/679/2016);
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati" **-** Articolo 5, paragrafo 1, lett. c), Reg. UE/679/2016);
- esatti e, se necessario, aggiornati. Devono, inoltre, essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati ("esattezza" - Articolo 5, paragrafo 1, lett. d), Reg. UE/679/2016);
- 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 ("limitazione della conservazione" - Articolo 5, paragrafo 1, lett. e), Reg. UE/679/2016);
- trattati in modo da garantire un'adeguata sicurezza dei dati personali attraverso l'adozione di tutte le misure, tecniche e organizzative, ritenute idonee a salvaguardare la correttezza del processo di raccolta e gestione dei dati, nonché la loro sicurezza e protezione in caso di intrusioni e alterazioni non autorizzate ("integrità e riservatezza" Articolo 5, paragrafo 1, lett. f), Reg. UE/679/2016);
- trattati secondo un sistema di gestione del rischio *privacy* che individui i rischi connessi al trattamento, li valuti in termini di origine, natura, probabilità e gravità definendo le migliori prassi per attenuare il rischio connesso ad ogni trattamento eseguito. L'adeguatezza delle misure adottate per ogni trattamento è valutata *ex ante*, secondo una prospettiva preventiva, ed *ex post*, a seguito di eventuali mutamenti del contesto di riferimento ("accountability" - Articolo 24, Reg. UE/679/2016).

Accountability ed elementi del sistema di gestione

L'articolo 24, Reg. UE 2016/679 prevede che il Titolare del trattamento metta in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Reg. UE 2016/679, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

Tale disposizione si traduce nel cosiddetto principio di accountability (responsabilizzazione). Al fine di rispettare il principio di accountability e gli ulteriori principi applicabili al trattamento già menzionati, AREU provvede all'implementazione, sviluppo e mantenimento di un sistema di gestione privacy che possa garantire l'integrazione nel trattamento di dati personali delle misure tecniche e organizzative necessarie a soddisfare i requisiti normativi e i diritti degli interessati fin dalle fasi iniziali del trattamento di dati personali ("privacy by design" - Articolo 25, Reg. UE/679/2016).

Il sistema di gestione privacy è un modello organizzativo fatto di politiche, procedure, persone e attività che garantiscono l'integrazione sistematica dei requisiti previsti dalla normativa privacy (europea e/o nazionale).

Il sistema di gestione per la protezione dei dati di AREU si compone dei ruoli, funzioni ed elementi descritti nel proseguo della presente Politica Generale per la Protezione dei Dati Personali.

Ruoli del sistema di gestione per la protezione dei dati

Le figure coinvolte nel sistema di gestione protezione dati di AREU sono quelle di seguito elencate:

- Titolare del Trattamento
- Contitolari del trattamento
- Data Protection Officer
- S.C. Affari Generali e Legali
- S.C. Sistemi informativi
- Referenti privacy di Struttura e soggetti autorizzati al trattamento
- Gruppo di Lavoro Privacy
- Responsabili e sub-responsabili del Trattamento

Titolare del trattamento

AREU, rappresentata ai fini previsti del GDPR dal Direttore Generale pro-tempore (rappresentante legale), è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare").

Il Titolare determina le finalità e i mezzi del trattamento dei dati personali ed è dotato di un potere decisionale in ordine alle misure tecniche ed organizzative da adottare con riferimento a tutte le operazioni di trattamento eseguite.

AREU in quanto Titolare del trattamento provvede a:

i. definire finalità e mezzi del trattamento di dati personali e le categorie di dati trattati;

ii. adottare tutte le misure tecniche ed organizzative necessarie per garantire il rispetto dei principi applicabili al trattamento (liceità, correttezza e trasparenza, limitazione delle finalità, minimizzazione dei dati, esattezza, limitazione della conservazione), la tutela dei diritti dei soggetti interessato e la sicurezza dei dati trattati (riservatezza, integrità, disponibilità dei dati e resilienza dei sistemi di trattamento);

iii. verificare ed aggiornare periodicamente le misure tecniche ed organizzative adottate;

iv. scegliere i soggetti coinvolti nel trattamento in base alle garanzie offerte per il rispetto dei principi di cui al Reg. UE 2016/679 e istruirli adeguatamente in merito al trattamento;

v. in caso di violazioni di dati personali, attuare contro-misure tempestive ed effettive a mitigare le conseguenze per i soggetti interessati, nonché valutare adeguatamente i rischi per gli stessi ed effettuare le comunicazioni dovute ai sensi di legge.

Il Titolare adotta misure appropriate per fornire all'interessato:

i) le informazioni indicate dall'art. 13 GDPR, qualora i dati personali siano raccolti presso lo stesso interessato;

ii) le informazioni indicate dall'art. 14 GDPR, qualora i dati personali non siano stati ottenuti presso lo stesso interessato.

Il Titolare, inoltre, provvede a:

i. individuare i Referenti Privacy di Struttura nelle persone dei Dirigenti/Responsabili delle singole strutture in cui si articola l'organizzazione aziendale;

ii. nominare il Responsabile della protezione dei dati – Data Protection Officer ("DPO");

iii. nominare, quale Responsabile esterno del trattamento (ai sensi dell'articolo 28 GDPR), ogni persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratti dati personali per conto dell'Agenzia in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali.

Contitolari del trattamento

Ogni qualvolta AREU determini congiuntamente, insieme a uno o più titolari del trattamento, le finalità e i mezzi del trattamento, i soggetti coinvolti sono contitolari del trattamento.

I Contitolari determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati.

Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata all'Agenzia da enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'art. 26 GDPR.

L'accordo definisce le responsabilità di ciascuno in merito all'osservanza degli obblighi in tema di privacy, con particolare riferimento all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del GDPR, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile.

Data Protection Officer

Il Data Protection Officer "DPO", è colui a cui è affidato il compito di osservare, valutare e supportare il Titolare nella gestione del sistema *privacy*, affinché i dati personali siano trattati nel rispetto delle disposizioni europee e nazionali.

In particolare, il DPO ha il compito di:

i. informare e fornire consulenza al Titolare nonché ai dipendenti degli obblighi derivanti dal GDPR;

ii. sorvegliare l'osservanza del GDPR, nonché delle altre disposizioni europee o di diritto interno in materia di protezione dati;

iii. sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e attività di controllo;

iv. fornire supporto alla S.C. Affari Generali e alla S.C. Sistemi Informativi per l'analisi e per la risoluzione operativa di specifiche problematiche connesse al trattamento di dati personali;

v. fornire pareri e sorvegliare sulla redazione del *Data Protection Impact Assessment* (c.d. DPIA);

vi. fungere da punto di contatto e collaborare con l'Autorità Garante per la protezione dei dati personali;

vii. assicurarsi che le violazioni dei dati personali siano documentate, notificate e comunicate.

AREU assicura che il DPO sia coinvolto tempestivamente e adeguatamente in tutte le questioni riguardanti la protezione dei dati personali e che mantenga la propria posizione d'indipendenza e imparzialità, come previsto dall'articolo 38, Reg. UE 2016/679.

AREU assicura inoltre che il DPO non riceva alcuna istruzione per quanto riguarda l'esecuzione dei suoi compiti, né che venga rimosso o penalizzato per l'adempimento dei propri compiti. Il DPO riferisce direttamente al vertice gerarchico di AREU.

Nell'esercizio delle proprie mansioni, il DPO sottopone il sistema di gestione per la protezione dei dati e il trattamento di dati personali ad *audit periodici* atti ad accertare l'effettivo rispetto del Reg. UE 2016/679, del Codice Privacy e di ogni provvedimento dell'Autorità Competente.

S.C. Affari Generali e Legali

AREU individua, quale organo di coordinamento del sistema per la protezione dei dati e per l'attuazione della presente Politica Generale la S.C. Affari Generali e Legali.

La S.C. Affari Generali e Legali cura i processi di predisposizione, verifica, approvazione, emissione e pubblicazione della documentazione privacy (regolamenti, linee guida, procedure o modelli aziendali) necessari all'attuazione del sistema di gestione per la protezione dei dati e della presente Politica Generale.

La S.C. Affari Generali è inoltre il punto di contatto e coordinamento tra il DPO e la SC Sistemi Informativi, al fine di coadiuvare e supportare i Referenti privacy interni nelle misure di adeguamento al GDPR.

La S.C. Affari Generali e Legali inoltre:

i. cura la predisposizione delle proposte di deliberazione alla Direzione Generale per la formale adozione di Regolamenti "privacy", di carattere generale;

ii. cura la pubblicazione sul sito internet aziendale di documenti afferenti alla Politica Generale per la Protezione dei Dati Personali;

iii. svolge in generale una funzione di filtro e, nei casi più complessi, di facilitazione, anche favorendo i rapporti tra soggetti del modello organizzativo ed il Gruppo di lavoro privacy e/o il DPO;

iv. cura la compilazione, la tenuta e l'aggiornamento del Registro delle attività di trattamento aziendale.

S.C. Sistemi informativi

La S.C. Sistemi informativi contribuisce all'efficiente e sicuro svolgimento delle attività dell'Agenzia attraverso definizione dell'architettura informativa dell'Agenzia e rendendo tecnologicamente possibile e governabile lo scambio di informazioni di tipo strutturale, logistico e clinico correlate a tutte le attività svolte o coordinate da AREU.

La S.C. Sistemi Informativi collabora con la S.C. Affari Generali e Legali e con il Data Protection Officer nella gestione di ogni violazione di dati personali (c.d. "data breach") ai sensi degli artt. 33 e 34 del Reg. Ue 2016/679. La S.C. Sistemi Informativi è responsabile dello svolgimento delle azioni di contenimento e mitigazione delle conseguenze di una violazione di dati personali, nonché del ripristino dei sistemi informativi e dei database coinvolti, come meglio previsto dalla successiva Sezione "Violazioni di Dati Personali" della presente Politica Generale.

Alla S.C. Sistemi Informativi è inoltre affidato il coordinamento del Gruppo di Lavoro sulla Cybersicurezza, viste le specifiche competenze e professionalità possedute nella materia.

La S.C. Sistemi Informativi e il Gruppo di Lavoro sulla Cybersicurezza collaborano con la S.C. Affari Generali e Legali e con il Gruppo di Lavoro Privacy al fine di gestire al meglio ogni rischio derivante dal trattamento di dati personali e da potenziali incidenti di sicurezza da cui potrebbe derivarne una perdita di riservatezza, integrità e disponibilità.

Referenti privacy di Struttura

Il ruolo di Referente privacy di Struttura è attribuito ai Direttori di Dipartimento, Dirigenti/Referenti delle singole Strutture in cui si articola l'organizzazione aziendale. I Referenti privacy sono dunque i soggetti dell'organizzazione aziendale a cui vengono affidati specifici compiti in materia di protezione dei dati personali come di seguito declinati.

Osservare e fare osservare:

i. le policy aziendali in materia di protezione dei dati fornite dal Titolare del trattamento;

ii. le istruzioni di carattere specifico impartite dal Titolare alle Strutture, in merito a specifici trattamenti, anche ad alto rischio;

iii. le istruzioni di carattere generale impartite dal Titolare a tutti i soggetti autorizzati al trattamento dei dati personali ai sensi dell'art. 2-quaterdecies del Codice Privacy.

Inoltre:

i. designare i soggetti autorizzati al trattamento dei dati personali, attraverso la predisposizione di apposito format aziendale;

ii. vigilare sulla conformità dell'operato dei soggetti autorizzati, ad essi afferenti, alle istruzioni e alle policy aziendali;

iii. verificare che i dati oggetto di trattamento siano esatti, aggiornati, indispensabili, pertinenti e non eccedenti rispetto alle finalità per cui vengono trattati;

iv. attenersi alle misure di sicurezza definite dalla S.C. Sistemi Informativi;

v. partecipare ai momenti formativi organizzati dall'Agenzia ed assicurare la partecipazione dei soggetti autorizzati;

vi. collaborare con la S.C. Affari Generali e Legali, con il DPO e con il Gruppo di lavoro privacy e fornire, quando richiesto, ogni informazione relativa al trattamento di dati personali realizzato dalla propria Struttura;

vii. segnalare ogni potenziale violazione della normativa in materia di protezione dei dati e trasmettere tempestivamente alla S.C. Affari Generali e Legali ogni informazione rilevante;

viii. segnalare tempestivamente le istanze e i reclami degli interessati pervenuti alla propria Struttura alla S.C. Affari Generali e Legali e al DPO;

ix. comunicare tempestivamente, e non oltre 24 ore dalla scoperta, alla S.C. Affari Generali e Legali, ogni incidente di sicurezza da cui possa derivare una violazione di dati personali di cui si viene a conoscenza, avendo cura di indicare le informazioni e gli elementi descritti nella presente Politica Generale (Sez. Violazioni dati personali);

x. comunicare alla S.C. Affari Generali e Legali l'inizio di ogni nuovo trattamento e la cessazione o modifica di quelli esistenti, ai fini della compilazione e del continuo aggiornamento del Registro delle attività di trattamento aziendale;

xi. assicurare che a ogni Responsabile del trattamento sia sottoposto l'atto di designazione a norma dell'articolo 28 del Reg. UE 2016/679, così come predisposto dalla S.C. Affari Generali e Legali, avendo cura di mantenerne copia firmata;

xii. avere cura di compilare e mantenere aggiornato l'elenco dei Responsabili del trattamento che trattano dati per la propria Struttura, così come predisposto dalla S.C. Affari Generali e Legali in formato elettronico;

xiii. collaborare con la S.C. Affari Generali e Legali nel processo di valutazione di impatto dei trattamenti ad alto rischio, qualora ne ricorrano i presupposti in base all'art.35 del GDPR e così come definito nella presente Politica Generale (Sez. Gestione dei rischi per i diritti e libertà dei soggetti interessati);

xiv. astenersi dal realizzare trattamenti di dati personali diversi e ulteriori senza la preventiva autorizzazione del Titolare del trattamento.

Gruppo di lavoro privacy

Il Gruppo di lavoro privacy, costituito con Delibera del Direttore Generale 94/2023, ha il compito di supportare AREU nell'applicazione interna del GDPR e del sistema di gestione privacy così come definito dalla presente Politica Generale. Il Gruppo di lavoro privacy assicura una gestione

integrata e coordinata a livello aziendale del sistema di gestione privacy e della sicurezza delle informazioni in tutti i processi operativi.

Il Gruppo di lavoro privacy è il punto di riferimento per l'elaborazione e per l'applicazione di tutte le procedure e processi necessari alla corretta implementazione del sistema di gestione aziendale privacy e per la sicurezza delle informazioni, in raccordo con la S.C. Sistemi Informativi e il gruppo di lavoro sulla cybersicurezza.

Sotto il coordinamento della S.C. Affari Generali e Legali, il Gruppo di lavoro privacy si occupa anche di agevolare lo svolgimento di valutazioni d'impatto per ogni ipotesi di trattamento di dati personali che coinvolga più di una Struttura.

Soggetti autorizzati al trattamento

Chiunque abbia accesso o sia chiamato a trattare dati personali sotto l'autorità e direzione di AREU è formalmente autorizzato e istruito dalla stessa in merito al trattamento. Sono qualificabili come soggetti autorizzati al trattamento, oltre ai dipendenti, anche specializzandi, tirocinanti, volontari e tutti coloro che a qualsiasi titolo svolgono attività di trattamento di dati personali sotto la direzione di AREU.

I soggetti autorizzati al trattamento devono rispettare la presente Politica Generale per la Protezione dei Dati Personali, nonché ogni altra istruzione impartita da AREU, anche attraverso procedure interne e istruzioni specifiche.

Al momento dell'assunzione di nuovi dipendenti, o comunque al momento dell'inizio dell'attività di specializzandi, tirocinanti, volontari e ogni altro soggetto che svolge attività di trattamento sotto la direzione di AREU, vengono fornite specifiche istruzioni attraverso apposito atto di autorizzazione, sottoscritto dal Direttore di Dipartimento/delle singole strutture.

Ogni soggetto autorizzato al trattamento ha l'obbligo di operare con la massima diligenza e attenzione in tutte le fasi di trattamento, al fine di garantire l'esatta acquisizione dei dati, il loro costante aggiornamento e un'adeguata conservazione.

Tra i doveri di ogni soggetto autorizzato, vi sono:

i. garantire la massima riservatezza in ogni fase del trattamento di dati personali;

ii. trattare i dati esclusivamente per le finalità previste e per quanto necessario per lo svolgimento della propria mansione;

iii. osservare scrupolosamente le indicazioni fornite in apposite politiche, procedure interne e manuali;

iv. osservare le istruzioni fornite nell'atto di autorizzazione al momento d'assunzione o di inizio della propria attività presso AREU.

Responsabili e Sub Responsabili del trattamento

Il Responsabile del trattamento, fornitore/consulente, è il soggetto che svolge attività di trattamento di dati personali per conto del Titolare.

L'Agenzia, qualora si avvalga di soggetti esterni per lo svolgimento di servizi nell'ambito dei quali sia necessario eseguire un trattamento di dati personali, nomina il prescelto fornitore/consulente quale Responsabile del trattamento.

L'incarico è sempre affidato tramite contratto o altro atto giuridico vincolante contenente almeno gli elementi elencati all'art. 28 del Reg. UE 2016/679.

È compito di ciascun Referente privacy di Struttura assicurare che ogni soggetto esterno che svolga un trattamento di dati personali per conto della Struttura e di AREU sia nominato come

Responsabile del trattamento. Ogni Referente privacy di Struttura trasmette alla S.C. Affari Generali e Legali evidenza di tale designazione, anche ai fini dell'aggiornamento del Registro delle attività di trattamento.

L'elenco aggiornato dei Responsabili del trattamento nominati è tenuto a cura di ciascun Referente privacy di Struttura.

I contratti o gli altri atti giuridici vincolanti ai sensi dell'art. 28 del Reg. UE 2016/679 contengono sempre almeno clausole che definiscano i seguenti elementi:

i. autorizzazione generale a incaricare sub-responsabili del trattamento, con obbligo di comunicazione degli stessi ad AREU;

ii. obbligo, per il Responsabile del trattamento, di agire soltanto su istruzione documentata del titolare, salvo obblighi di legge;

iii. obbligo, per il Responsabile del trattamento, di assistere il titolare nel rispetto degli adempimenti di cui agli artt. 15-22, artt. 33-34, art. 35 del Reg. UE 2016/679;

iv. obbligo, per il Responsabile del trattamento, di sottoporsi ad audit e ispezioni, anche documentali, da parte del Titolare.

I Referenti Privacy di Struttura, in concerto con la S.C. Affari Generali e Legali, valutano l'opportunità di inserire nei contratti clausole rescissorie o penali in caso di violazione della normativa o delle istruzioni rese dal Titolare, anche in base alla natura del trattamento e al relativo rischio per i diritti e libertà dei soggetti interessati.

Gestione del Registro del trattamento di dati personali e mappatura periodica

Il Registro delle attività di trattamento dati contiene le informazioni relative alle operazioni di trattamento eseguite dall'Agenzia in qualità di Titolare e/o Responsabile del trattamento.

La presente sezione descrive la struttura del Registro adottato internamente, come previsto dall'art. 30 del Reg. UE 2016/679 (GDPR), nonché le modalità per la mappatura periodica del trattamento dati e per l'aggiornamento periodico del Registro.

Struttura e gestione del Registro

Il Registro del trattamento di dati personali è mantenuto da AREU in formato elettronico, anche attraverso l'ausilio di software specialistici. Il Registro viene conservato e mantenuto aggiornato dalla S.C. Affari Generali e Legali, che mette a disposizione lo stesso in caso di richiesta da parte dell'Autorità Competente.

Il Registro descrive almeno i seguenti elementi per ogni trattamento di dati personali:

i. Struttura di riferimento

ii. Nome del trattamento / descrizione

iii. Finalità del trattamento

iv. Basi giuridiche ai sensi degli artt. 6, 9, 10 del Reg. UE 2016/679

v. Tempi di conservazione

Aggiornamento periodico del Registro

Il Registro è aggiornato periodicamente, almeno una volta l'anno, oppure a seguito di ogni nuova mappatura totale o parziale di dati personali.

In ogni caso, il Registro è aggiornato ogni qualvolta sopravvenga almeno una delle seguenti condizioni:

i. modifica dei sistemi di elaborazione e/o archiviazione di dati personali, come sistemi di posta elettronica, software per la gestione delle risorse umane, software per la gestione della formazione, sistemi di archiviazione (anche in Cloud);

ii. cambiamenti nell'assetto organizzativo aziendale;

iii. modifica dei soggetti terzi coinvolti nelle attività di trattamento, come responsabili del trattamento e altri titolari;

iv. nuove attività di trattamento dati o modifica delle caratteristiche delle attività di trattamento già censite.

Il Registro viene mantenuto aggiornato in tutte le sue parti, avendo cura di indicare anche la data di ultima modifica.

Gestione dei rischi per i diritti e libertà dei soggetti interessati

Nel caso in cui un trattamento di dati personali, specie se prevede l'uso di nuove tecnologie possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve effettuare una valutazione d'impatto sulla protezione dei dati ("DPIA") ai sensi dell'art. 35 GDPR, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento.

Valutazione d'impatto (DPIA)

La valutazione d'impatto per la protezione dei dati (DPIA) è un processo che ha lo scopo di identificare, valutare e gestire i rischi per i soggetti interessati derivanti dal trattamento dei loro dati personali, nonché valutare la conformità del trattamento stesso.

La valutazione d'impatto è un elemento chiave del GDPR e deve essere eseguita prima dell'avvio di un trattamento di dati che potrebbe comportare rischi elevati per i diritti e le libertà dei soggetti interessati. Durante questo processo, vengono identificati i rischi, valutate le misure di mitigazione e sviluppate strategie per garantire la conformità alle norme privacy nazionali ed europee, nonché alle politiche interne di AREU.

La valutazione d'impatto per la protezione dei dati comprende diverse fasi, tra cui la descrizione del trattamento e ciclo di vita dei dati, la valutazione della necessità e proporzionalità del trattamento, l'analisi dei rischi, l'identificazione delle misure di mitigazione degli stessi e il parere del DPO in merito al processo di DPIA. Il piano di miglioramento per introdurre le misure necessarie a mitigare i rischi può essere contenuto nella valutazione d'impatto o essere prodotto come allegato separato.

L'obiettivo finale è quello di ridurre al minimo i rischi per la privacy e garantire un trattamento adeguato e sicuro dei dati personali, conformemente ai principi fondamentali del GDPR.

Obbligatorietà della valutazione d'impatto

La valutazione d'impatto è obbligatoria in tutti i casi previsti per legge. In particolare, è obbligatorio sottoporre un trattamento di dati personali a valutazione d'impatto quando ricorrano due o più dei seguenti criteri:

i. valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione di comportamenti o abitudini;

ii. processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente sui soggetti interessati;

iii. monitoraggio sistematico dei soggetti interessati;

iv. trattamento di dati sensibili o dati aventi carattere altamente personale;

v. trattamento di dati su larga scala;

vi. creazione di corrispondenze o combinazione di insiemi di dati;

vii. trattamento di dati relativi a soggetti interessati vulnerabili (es. malati, minori, invalidi, ecc.);

viii. uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative;

ix. il trattamento impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio.

La valutazione d'impatto è inoltre obbligatoria in tutti i casi specificatamente definiti con Provv. N. 467/2018 dell'Autorità Garante per la Protezione dei Dati personali, pubblicato in G.U. n. 269 del 19 novembre 2018.

Fasi di una valutazione d'impatto

La valutazione d'impatto (DPIA) si compone di diverse fasi:

i. Identificazione del trattamento dei dati: descrivere il trattamento dei dati personali che AREU intende effettuare, specificando le finalità, le categorie di dati coinvolti, i soggetti interessati, il tempo di conservazione e i destinatari dei dati;

ii. Valutazione della necessità e proporzionalità: verificare se il trattamento dei dati è necessario per il raggiungimento delle finalità previste e se è proporzionato rispetto agli obiettivi da perseguire, nonché verifica dell'esistenza delle corrette basi giuridiche;

iii. Valutazione dei rischi per i soggetti interessati e della potenziale violazione o limitazione dei loro diritti e libertà: identificare e valutare i potenziali rischi che il trattamento dei dati può comportare per i diritti e libertà degli individui, compresi quelli derivanti da incidenti di sicurezza come divulgazione non autorizzata, perdita dei dati o uso improprio;

iv. Identificazione misure di mitigazione e piano di miglioramento: identificare le misure tecniche e organizzative necessarie per ridurre i rischi individuati durante l'analisi e preparare un piano di miglioramento con assegnazione delle responsabilità e tempi per l'implementazione delle misure di mitigazione.

Le valutazioni d'impatto devono essere aggiornate nel momento in cui ci sia un cambiamento nel trattamento analizzato da cui possa derivare un impatto sui diritti e le libertà dei soggetti interessati. La documentazione della valutazione d'impatto riporta sempre data, versione e storico degli ultimi aggiornamenti.

A conclusione di ogni valutazione d'impatto il Data Protection Officer rende il suo parere documentato in merito al processo e alle valutazioni effettuate.

Iter per lo svolgimento di valutazioni d'impatto

La valutazione d'impatto è un processo complesso che viene svolto in collaborazione tra la Struttura interessata dal trattamento e il Gruppo di lavoro privacy, con il coordinamento della S.C. Affari Generali e Legali.

Ogni Referente Privacy di Struttura ha la responsabilità di informare, con congruo preavviso, la S.C. Affari Generali e Legali della volontà di iniziare un trattamento di dati personali da cui potrebbe derivare un rischio elevato per i diritti e libertà dei soggetti interessati. Il trattamento si presume comportare un rischio elevato ogni qualvolta ricorrano due o più degli elementi indicati nella precedente sezione.

Valutazione dei rischi della filiera del dato

Nel rispetto del principio di accountability e come previsto dall'art. 28 del Reg. UE 2016/679, è responsabilità e onere di AREU ricorrere unicamente a Responsabili del trattamento in grado di mettere in atto misure tecniche e organizzative adeguate a far sì che il trattamento di dati personali a loro affidato possa soddisfare i requisiti normativi e le politiche interne.

AREU si impegna a integrare i processi di ricerca e selezione di fornitori o altri soggetti qualificabili come Responsabili del trattamento in modo tale da poter valutare e mitigare preventivamente possibili rischi derivanti dal trattamento di dati realizzato da questi soggetti.

Elementi per la valutazione dei Responsabili del trattamento e dei rischi

I Responsabili del trattamento sono selezionati da AREU anche in ragione delle garanzie offerte per la protezione dei dati e del rispetto dei requisiti di conformità previsti dal Reg. UE 2016/679.

La selezione e valutazione delle garanzie offerte viene svolta dalle Strutture competenti per l'assegnazione del servizio, anche attraverso appositi questionari o allegati tecnici da sottoporre ai partecipanti alla gara.

Il Responsabile del trattamento è valutato tenendo conto dei seguenti elementi:

i. processi: il fornitore dovrebbe essere in grado di dimostrare l'esistenza di processi per la gestione conforme e sicura dei dati personali, nonché per la gestione delle violazioni e degli incidenti di sicurezza;

ii. persone: il fornitore dovrebbe essere in grado di dimostrare la formazione delle persone in tema di protezione dei dati personali e di buone prassi per la sicurezza degli stessi;

iii. tecnologie: i sistemi informativi e i servizi informatici utilizzati dal fornitore dovrebbero essere adeguatamente sicuri, in grado di garantire la conformità alla normativa e predisposti per l'esercizio dei diritti sui dati;

iv. certificazioni: eventuale possesso di certificazioni rilevanti per la conformità e sicurezza del trattamento di dati personali.

Se necessario, i Referenti Privacy consultano la S.C. Affari Generali e Legali e/o la S.C. Sistemi Informativi al fine di ottenere supporto nella valutazione dei Responsabili del trattamento.

Monitoraggio dei Responsabili del trattamento

I Responsabili del trattamento possono essere sottoposti a periodiche verifiche a campione al fine di assicurare che il trattamento di dati personali venga svolto in conformità con quanto previsto dal Reg. UE 2016/679 e dalle istruzioni fornite contrattualmente.

La specifica natura delle verifiche è descritta negli atti di cui all'articolo 28 Reg. UE 2016/679.

Principio di limitazione della conservazione

L'art. 5, paragrafo 1, lett. e) del Reg. UE 2016/679 prescrive che i dati personali siano "*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*". Il criterio principale da utilizzare per determinare la durata del trattamento è sempre la necessità dei dati per il raggiungimento delle finalità perseguite.

Nel definire i tempi di conservazione dei dati è quindi necessario tenere in considerazione e diversificare le diverse finalità per cui sono trattati oppure, qualora esistenti, tenere in considerazione specifici obblighi di legge che impongono un certo periodo di conservazione.

Ciclo vita dei dati

I dati trattati da AREU seguono il seguente ciclo di vita:

i. creazione: creazione/acquisizione dei dati, sia interna che esterna, e conservazione

ii. distribuzione: gestione delle informazioni e distribuzione interna / esterna

iii. uso: elaborazione delle informazioni nei processi di business

iv. manutenzione: archiviazione, recupero, e trasferimento di informazioni

v. distruzione: processo di gestione delle informazioni meno usate o alla fine del loro periodo di retention.

Tempi di conservazione

I termini di conservazione dei dati personali trattati da AREU sono disciplinati dalla normativa regionale, come indicato dalla DGR n. 4659 del 9 gennaio 2013 e successive. In particolare, tale normativa disciplina le modalità di gestione, archiviazione e cancellazione/distruzione.

In particolare, il "Titolario e massimario di scarto" disciplina il ciclo di vita che i documenti hanno dal momento della loro produzione sino all'eventuale scarto. Questo documento, poiché ordina e classifica tutta la documentazione sanitaria e sociosanitaria è oggetto di periodiche revisioni da parte della Regione Lombardia.

I tempi di conservazione dei sono indicati nel Registro delle attività di trattamento predisposto da AREU ai sensi dell'articolo 30 del Reg. UE 2016/679.

Archiviazione dei dati

I soggetti autorizzati al trattamento hanno il dovere di evitare la frammentazione e dispersione delle banche dati di AREU, che renderebbero più difficoltosa la tracciabilità e conseguente cancellazione/anonimizzazione dei dati personali non più necessari.

Ogni soggetto autorizzato al trattamento è pertanto tenuto a rispettare le misure tecniche e istruzioni fornite dalla S.C. Sistemi Informativi al fine di conservare nel modo più adeguato dati e documenti contenenti dati personali.

Sicurezza dei dati personali

La S.C. Sistemi Informativi è responsabile della sicurezza dei dati personali trattati da AREU a livello tecnico e informatico. In ogni caso, l'Agenzia assicura l'adozione di misure tecniche e organizzative tali da garantire un livello di sicurezza adeguato al rischio per i diritti e libertà dei soggetti interessati, tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto e del contesto del trattamento di dati personali.

AREU adotta almeno le seguenti misure per la sicurezza dei dati trattati:

i. autenticazione degli utenti che accedono ai sistemi informativi, anche multi-fattore ove necessario;

ii. adozione di politiche di controllo degli accessi e di restrizione dei diritti di accesso sulla base del principio di minimo privilegio;

iii. adozione di misure tecniche e organizzative per il backup e ripristino dei dati in caso di incidente da cui derivi una perdita di disponibilità o integrità degli stessi;

iv. protezione dei sistemi informativi elettronici attraverso sistemi (software e hardware) per l'individuazione di anomalie, malfunzionamenti e tentativi di attacco.

Se necessario, la S.C. Sistemi Informativi predispone una Politica Generale per la Cybersicurezza in cui siano definiti e resi noti ruoli e responsabilità del personale e delle Strutture, nonché le misure tecniche e organizzative inerenti alla cybersicurezza. Tale Politica Generale potrà essere integrata o separata rispetto alla presente.

Al fine di migliorare la sicurezza della filiera del trattamento di dati, la S.C. Sistemi Informativi collabora con la S.C. Affari Generali e Legali per definire le misure di sicurezza minime richieste a soggetti esterni che accedono a dati personali di cui AREU è Titolare, o che comunque svolgono trattamento di dati personali per conto di AREU, nel rispetto di quanto previsto dall'articolo 28 del Reg. UE 2016/679.

Violazioni di dati personali

Una violazione dei dati personali, secondo il Regolamento Generale sulla Protezione dei Dati (Reg. UE/679/2016), è un incidente di sicurezza che porta alla distruzione, perdita, alterazione, divulgazione non autorizzata o accesso, accidentale o illecito, a dati personali trasmessi, conservati o altrimenti elaborati. Tale violazione può compromettere la riservatezza, l'integrità o la disponibilità dei dati personali.

A titolo esemplificativo, sono considerati casi di violazione dei dati personali i seguenti scenari:

i. accesso o acquisizione non autorizzata di dati da parte di terzi;

ii. furto o perdita di dispositivi informatici o documenti cartacei contenenti dati personali;

iii. alterazione intenzionale dei dati personali; incapacità di accedere ai dati a causa di cause accidentali o attacchi esterni, come virus, malware, ecc.;

iv. perdita o distruzione dei dati personali a causa di incidenti, eventi avversi, incendi o altre catastrofi;

v. divulgazione non autorizzata di dati personali.

Obbligo di notifica e termini di legge

L'articolo 33 del Reg. UE 2016/679 prevede che il Titolare del trattamento debba notificare all'Autorità di controllo ogni violazione di dati personali entro 72 ore dalla sua scoperta, salvo che non sia improbabile che da tale violazione possa derivare un rischio per i diritti e libertà delle persone fisiche.

Le notifiche fatte oltre il termine di 72 ore devono essere accompagnate dalle ragioni del ritardo.

Nel caso in cui dalla violazione dei dati possa derivare un elevato rischio per i diritti e libertà delle persone fisiche, il Titolare del trattamento deve comunicarlo a tutti i soggetti interessati, utilizzando i canali ritenuti più adatti al contesto, come previsto dall'articolo 34 del Reg. UE 2016/679.

Segnalazione interna di eventi da cui possano derivare violazioni di dati

Chiunque ne abbia notizia segnala tempestivamente (e comunque entro e non oltre 24 h) alla S.C. Affari Generali e Legali ogni evento da cui possa derivare, anche solo potenzialmente, una violazione di dati personali, utilizzando l'apposita modulistica interna e avendo cura di comunicare almeno le seguenti informazioni essenziali:

i. nome e informazioni di contatto della persona che ha scoperto l'evento;

ii. luogo, data e ora della scoperta dell'evento;

iii. una breve descrizione di ciò che si presume sia accaduto;

iv. se possibile, una stima della tipologia e quantità di dati e sistemi che si sospetta possano essere stati compromessi.

I Referenti privacy di Struttura inoltrano senza ingiustificato ritardo il modulo di segnalazione alla S.C. Affari Generali e Legali, integrando, se del caso, ulteriori informazioni riguardanti l'evento. La S.C. Affari Generali e Legali provvede a esaminare la segnalazione interna dell'evento in base alle informazioni ricevute.

Fasi di gestione delle segnalazioni di violazione di dati

Gli eventi da cui possano derivare violazioni di dati, e le violazioni di dati confermate sono gestite da AREU e dai diversi responsabili nel rispetto delle specifiche procedure interne e delle seguenti fasi di gestione:

i. segnalazione interna: identificazione e segnalazione interna di un evento da cui possa derivare una violazione di dati;

ii. comprensione e valutazione gravità: comprensione della violazione di dati e valutazione della gravità della stessa, ai fini dell'adempimento degli obblighi legali;

iii. contenimento e ripristino: mitigazione delle conseguenze negative dell'evento e attivazione dei piani e protocolli per il ripristino dell'operatività dei sistemi di AREU;

iv. notifica: notifica all'Autorità di controllo e, se necessario, ai soggetti interessati;

v. chiusura violazione: inserimento nel Registro delle violazioni di tutte le informazioni rilevanti:

- Data della violazione
- Natura della violazione
- Descrizione della violazione
- Numero di soggetti interessati coinvolti
- Stima della gravità della violazione
- Misure di mitigazione adottate
- Data della notifica all'Autorità (se necessario)
- Data della notifica ai soggetti interessati (se necessario)
- Data di chiusura della violazione

Trasparenza e rapporti con i soggetti interessati

La disciplina sulla trasparenza nelle pubbliche amministrazioni non solo è finalizzata a favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'uso delle risorse pubbliche, ma è anche uno strumento di tutela dei diritti dei cittadini, come anche sottolineato dal Reg. UE 2016/679.

La trasparenza è dunque un fattore fondamentale per svolgere un'attività amministrativa eticamente corretta e conforme alla normativa privacy europea, valorizzando inoltre la responsabilità (accountability) di AREU nei confronti dei cittadini e delle Autorità competenti.

Informative sul trattamento dati

AREU assicura che tutte le informazioni rilevanti in relazione al trattamento di dati personali siano fornite ai soggetti interessati nel momento in cui i dati sono acquisiti. Ove ciò non sia possibile, è assicurata la pubblicazione delle informazioni sul sito istituzionale dell'Agenzia in un formato facilmente accessibile e con linguaggio chiaro, conciso e facilmente comprensibile dal pubblico di riferimento.

Nel rispetto di quanto previsto anche dal PIAO, ogni Struttura dell'Agenzia è coinvolta nei processi necessari a garantire la trasparenza del trattamento di dati personali, anche per ciò che riguarda la condivisione delle informazioni necessarie per integrare e mantenere aggiornati i documenti informativi ("privacy policy") destinati ai soggetti interessati.

Gestione istanze dei soggetti interessati e reclami

AREU garantisce la gestione dei reclami e delle segnalazioni relative al trattamento di dati personali, nonché delle richieste di esercizio dei diritti previsti dagli artt. 15-22 del Reg. UE 2016/679, come segue

i. accesso: diritto di ottenere l'accesso ai dati e di ottenere ogni informazione rilevante circa il trattamento effettuato. I soggetti interessati hanno anche diritto, se richiesto, di ottenere copia gratuita dei dati trattati;

ii. portabilità: diritto di ottenere i dati personali in un formato standard elettronico interoperabile (esempio file.csv);

iii. rettifica e cancellazione: diritto di ottenere la rettifica dei dati, oltre che la loro cancellazione definitiva. La richiesta cancellazione non è accoglibile in determinati casi;

iv. opposizione e limitazione: diritto di opporsi al trattamento effettuato sulla base del legittimo interesse del Titolare e di ottenere la limitazione del trattamento;

v. decisioni automatizzate: diritto di non essere sottoposti a decisione 100% automatizzata che produca effetti giuridici (salvo eccezioni di legge).

Fasi di gestione di una richiesta di esercizio di uno o più diritti previsti dal Reg. UE 2016/679

Le istanze ricevute da AREU per l'esercizio dei diritti previsti dagli artt. 15-22 del Reg. UE 2016/679 sono gestite nel rispetto delle seguenti fasi:

i. Identificazione del soggetto interessato: identificazione della persona fisica da cui arriva la richiesta;

ii. esame della richiesta: esame della richiesta e valutazione dei presupposti per l'accoglimento;

iii. ricerca e individuazione dei dati interessati: ricerca di database, sistemi e documenti per individuare i dati oggetto della richiesta;

iv. riscontro al soggetto interessato: riscontro al soggetto interessato con indicazione delle azioni intraprese, consegna di copia dei dati (se necessario) o indicazione delle motivazioni per cui la richiesta è stata rigettata;

v. chiusura della richiesta: descrizione della richiesta nel Registro con indicazione degli elementi essenziali e dei tempi e modi di risposta.

Identificazione del soggetto interessato o del suo legale rappresentante

Prima di dar seguito ad ogni istanza di esercizio dei diritti previsti dagli artt. 15-22 del Reg. UE 2016/679 è necessario identificare il soggetto interessato, al fine di diminuire il rischio di diffusione di dati personali verso soggetti non autorizzati.

Nel caso in cui il soggetto richiedente affermi di essere anche il soggetto interessato, la sua identità deve essere valutata attraverso l'ottenimento di un documento d'identità e con il confronto dei dati a disposizione con le informazioni fornite dal richiedente. Nel caso in cui tali informazioni siano carenti, è possibile chiedere al soggetto richiedente di integrarle.

Qualora il soggetto richiedente affermi di essere un delegato del soggetto interessato, la sua identità deve essere valutata attraverso l'ottenimento di un documento d'identità del soggetto interessato, del soggetto delegato e di una delega firmata.

Laddove il richiedente abbia omesso di fornire sufficienti informazioni sulla sua identità o l'identificazione risulti difficoltosa, è necessario rispondere con una richiesta di maggiori informazioni, anche attraverso la comunicazione di documenti contenenti dati personali che possano essere confrontati con quelli già nella disponibilità di AREU.

Ulteriori documenti del sistema di gestione privacy

Insieme alla presente Politica Generale per la Protezione dei Dati Personali, concorrono alla struttura del sistema di gestione privacy AREU i seguenti documenti essenziali:

i. Registro trattamento dati personali (art. 30 GDPR)
ii. Registro delle violazioni (art. 33 GDPR)
iii. Registro istanze esercizio diritti GDPR (artt. 15-22 GDPR)
iv. Informative Privacy (artt. 13-14 GDPR)
v. Nomine Responsabili trattamento (art. 28 GDPR)
vi. Valutazioni d'impatto (art. 35 GDPR)
vii. Modulistica interna a supporto del sistema privacy