Comune di Porto Azzurro
Provincia di Livorno

Linee Guida per la gestione delle attività in materia di protezione dei dati personali

Sommario

1. OBIETTIVO DEL DOCUMENTO

Il presente documento ha la finalità di regolare in modo organico le modalità di gestione delle tematiche attinenti alla protezione dei dati personali all'interno del Comune di Porto Azzurro (di seguito, anche il "Comune").

Esso definisce in maniera puntuale ruoli, compiti e responsabilità dei soggetti coinvolti nelle attività di trattamento, assicurando che ogni operazione sia svolta nel rispetto della normativa vigente in materia di protezione dei dati personali e secondo principi di liceità, correttezza, trasparenza e sicurezza.

L'obiettivo è garantire un assetto organizzativo chiaro, idoneo a presidiare adeguatamente i trattamenti effettuati dal Comune e a prevenire eventuali violazioni, assicurando un livello di tutela coerente con il quadro normativo europeo e nazionale.

2. RIFERIMENTI NORMATIVI

Di seguito si riportano i principali riferimenti normativi in materia di protezione dei dati personali considerati nella predisposizione del presente documento:

- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016;
- Decreto Legislativo 30 giugno 2003, n.196 recante il "Codice in materia di protezione dei dati personali" ss.mm.ii.;
- Decreto Legislativo 10 agosto 2018, n. 101 "relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)";
- Guidelines on Personal data breach notification under Regulation 2016/679 - wp250 del WP29.
- Linee guida del Garante Privacy, provvedimento 15/05/2014 n° 243; privacy e trasparenza on line della Pa

3. PRINCIPALI RUOLI E RESPONSABILITÀ IN AMBITO PRIVACY

Incaricati al trattamento, in qualità di personale dipendente presso gli Uffici del Comune, hanno la responsabilità di:

- eseguire il trattamento dei dati all'interno delle attività di propria competenza, garantendo la riservatezza, disponibilità e integrità dei dati personali, in conformità ai principi del Codice Etico, alle procedure policy e linee guida aziendali di riferimento e alle istruzioni fornite dal proprio Responsabile;
- supportare il proprio Responsabile nelle attività afferenti alla gestione della richiesta di esercizio dei diritti privacy da parte dell'Interessato;
- supportare il proprio Responsabile interno nelle attività necessarie a garantire l'applicazione del principio di privacy by design e by default ogni qualvolta sia previsto, nell'ambito del proprio Ufficio, lo sviluppo di un nuovo processo/servizio/attività/iniziativa/strumento che comporta il trattamento di dati personali o la modifica (di scopo o delle modalità) di un trattamento di dati personali già esistente, archiviando la relativa documentazione predisposta, all'interno della cartella di rete predisposta;
- segnalare al proprio Responsabile interno eventuali inadeguatezze nel processo di trattamento dei dati personali, difformità rispetto alle procedure in materia di privacy ovvero potenziali data breach (in caso di urgenza, informa direttamente DPO), qualora ne venisse a conoscenza;
- supportare il Coordinatore Privacy nella gestione e valutazione del potenziale data breach.

Titolare del trattamento in persona del Sindaco pro-tempore o delegati del Titolare di cui al successivo paragrafo, hanno la responsabilità di:

- fornire agli Interessati l'informativa sul trattamento dei loro dati personali ai sensi degli artt. 13 e 14 del Regolamento e richiederne, ove necessario, il relativo consenso ai sensi dell'art. 7 del Regolamento;
- mettere in atto misure tecniche e organizzative adeguate per garantire per impostazione predefinita, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento, tenendo 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, garantendo il principio di accountability, ai sensi dell'art. 24 del Regolamento;

- nominare il DPO in conformità all'art. 37 del Regolamento;

I soggetti delegati per l'esercizio delle funzioni di titolare del trattamento (Responsabile Privacy) dei dati personali, ciascuno nel rispettivo ambito di competenza, inoltre hanno la funzione di:

- assicurare il rispetto di tutti gli obblighi previsti dal regolamento e dalla normativa nazionale in capo al titolare del trattamento;
- definire finalità, mezzi di trattamento e rispettive responsabilità in merito all'osservanza degli obblighi previsti anche in caso di contitolarità del dato personale ai sensi dell'art. 26 del regolamento;
- effettuare, ove necessario e prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali (DPIA), ai sensi dell'art. 35 del Regolamento;
- chiedere al DPO, per il tramite degli incaricati dell'Ufficio interessato, di fornire un parere in merito alla DPIA, ai sensi dell'art. 39 del Regolamento
- designare il personale autorizzato al trattamento dei dati personali condividendo tale scelta con il Coordinatore Privacy, fornendo adeguate istruzioni per il loro corretto trattamento;
- istruire chiunque agisca sotto la sua autorità nell'ambito del trattamento di dati personali;
- verificare la corretta predisposizione delle informative e curarne il costante aggiornamento.
- nominare, ove ritenuto necessario per la complessità dell'U.O., un «referente privacy» della struttura per il supporto all'esercizio delle funzioni di titolare del trattamento e alle attività di gestione degli adempimenti connessi alla protezione dei dati nonché come punto di contatto con il RPD;
- nominare, in considerazione del contratto o atto giuridico stipulato tra le parti, eventuali 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 Regolamento e garantisca la tutela dei diritti dell'interessato, definendo il perimetro di accountability e responsability mediante specifiche istruzioni in conformità all'art. 28 del Regolamento;

- far sottoporre al potenziale fornitore, già in fase contrattuale/pre-contrattuale, un questionario al fine di rilevare le informazioni utili a:
    - l'eventuale iter di designazione del fornitore come Responsabile esterno al trattamento dei dati personali;
    - la valutazione delle misure di sicurezza proposte, ove necessario;
    - l'indirizzamento delle attività per regolamentare, in modo che risulti compliant a quanto previsto dalla normativa in materia di protezione dei dati personali, l'eventuale trasferimento di dati in Paesi extra UE.
- adottare misure appropriate al fine di garantire l'esercizio dei diritti di coloro i cui dati personali sono oggetto di trattamento previsti agli articoli da 15 a 18 e da 20 a 22 del regolamento, secondo le Linee Guida di cui al presente atto;
- prendere in carico la richiesta, di procedere all'istruttoria e alla conseguente valutazione di concerto con il Coordinatore Privacy, ai fini del tempestivo riscontro all'interessato affinché le tempistiche di risposta siano in linea con i termini previsti dal Regolamento e le Linee Guida;
- gestire la richiesta di esercizio dei diritti privacy da parte dell'Interessato, di concerto con il Coordinatore Privacy, coinvolgendo e coordinando il DPO e gli uffici di pertinenza, procedendo all'istruttoria e alla conseguente valutazione ai fini del tempestivo riscontro all'Interessato affinché le tempistiche di risposta siano in linea con i termini previsti dal Regolamento;
- registrare l'istanza ricevuta nel Registro delle Istanze degli Interessati, facendo archiviare tutta la correlata documentazione;
- dare supporto al Coordinatore Privacy nella gestione dei data breach e nel processo di valutazione e di notifica al Garante della protezione dei dati personali delle violazioni dei dati personali (data breach) e provvedere alla comunicazione della violazione agli

interessati, ai sensi degli articoli 33 e 34 del Regolamento, secondo quanto disposto all'art. 9, e darne informativa preventiva alla Giunta, al Coordinatore Privacy e al RPD;

Coordinatore Privacy, in persona del Segretario Comunale, ha la responsabilità di:

- supporta i Responsabili Privacy nella gestione del trattamento dei dati personali nell'ambito delle strutture di loro competenze, oggetto di delega da parte del Titolare;
- gestire e valutare il potenziale data breach, con il supporto del DPO e del Responsabile Privacy delegato dal Titolare del trattamento;
- monitorare la completa e corretta attuazione da parte dei Responsabili, delle misure correttive individuate nell'ambito della valutazione del data breach, in considerazione delle scadenze previste, riferendo al Titolare del trattamento, con il supporto del DPO;
- predisporre la notifica da far sottoscrivere al Titolare, con il supporto del DPO ed eventuali Responsabili esterni del trattamento / specialisti esterni, così da inviarla al Garante per la protezione dei dati personali;
- registrare tutte le segnalazioni di un potenziale data breach pervenute all'interno del Registro Interno delle Violazioni, indipendentemente dalle notifiche che saranno effettuate a seguito della valutazione del data breach.

DPO, in qualità di Responsabile della protezione dei dati, ha la responsabilità di:

- informare e fornire consulenza al titolare del trattamento, ai Responsabili e al Coordinatore, in merito agli obblighi derivanti dal Regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- sorvegliare l'osservanza del Regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile 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;
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;

- cooperare con il Garante per la protezione dei dati personali;
- fungere da punto di contatto per il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;
- ricevere l'istanza dell'interessato nell'ambito dell'esercizio dei diritti privacy, come previsto da informativa, inoltrandola al Titolare del trattamento, al Responsabile o al Coordinatore supportando quest'ultimo, ove necessario, nella valutazione sulla fondatezza della richiesta;
- collaborare con il Coordinatore e con il Responsabile nella gestione delle attività necessarie a garantire l'applicazione del principio di privacy by design e by default ogni qualvolta sia previsto, nell'ambito del proprio Ufficio, lo sviluppo di un nuovo processo/servizio/attività/iniziativa/strumento che comporta il trattamento di dati personali o la modifica (di scopo o delle modalità) di un trattamento di dati personali già esistente
- supportare il Coordinatore nella gestione e valutazione del potenziale data breach;
- supervisionare la corretta implementazione delle misure disposte dal Garante per la protezione dei dati personali.

4. GESTIONE DELLE RICHIESTE DI ESERCIZIO DEI DIRITTI PRIVACY DA PARTE DEGLI INTERESSATI

4.1 Premessa

Gli Interessati possono esercitare, in qualunque momento, i diritti previsti agli artt.15, 16, 17, 18, 20, 21 e 22 del GDPR che conferiscono, in particolare, la facoltà di:

- ottenere dal Comune di Porto Azzurro, quale Titolare del trattamento, la conferma dell'esistenza di propri dati personali, ed in tal caso l'accesso agli stessi ed alle informazioni previste dall'articolo di riferimento;
- 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;

- ottenere dal Titolare del trattamento la cancellazione dei dati che lo riguardano, nei casi disciplinati dall'articolo di riferimento, senza ingiustificato ritardo;
- ottenere dal Titolare del trattamento la limitazione del trattamento quando ricorre una delle ipotesi disciplinate dall'articolo di riferimento;
- ottenere dal Titolare del trattamento la portabilità dei dati, ossia di ricevere in un formato strutturato, di uso comune e leggibile da un dispositivo automatico, i dati personali che lo riguardano e di trasmettere direttamente tali dati, se tecnicamente fattibile, ad un altro Titolare del trattamento senza impedimenti da parte del primo Titolare cui li ha forniti, qualora ricorrano le condizioni indicate dall'articolo di riferimento;
- opporsi in qualsiasi momento, in tutto o in parte, al trattamento dei dati personali che lo riguardano, a meno che non vi siano motivi legittimi per procedere al trattamento, nei casi espressamente disciplinati dall'articolo di riferimento;
- non essere sottoposto ad 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, ad eccezione di casi espressamente disciplinati dall'articolo di riferimento.

4.2 Ricezione dell'istanza

Le richieste relative all'esercizio dei diritti da parte dell'Interessato possono essere trasmesse tramite posta elettronica all'indirizzo PEC: comuneportoazzurro@pcert.it od anche inviando una istanza all'indirizzo del RPD/DPO alla email: privacy@comuneportoazzurro.li.it., dedicato alla ricezione delle istanze come definito all'interno delle informative privacy rilasciate. Nel momento in cui viene ricevuta una richiesta degli Interessati con riferimento all'esercizio di uno dei diritti ad essi riconosciuti ai sensi del Regolamento, il DPO la inoltra per conoscenza al Responsabile Privacy o al Coordinatore Privacy.

Qualora la richiesta da parte dell'Interessato pervenga ad altri destinatari attraverso qualsiasi altro mezzo (a titolo esemplificativo e non esaustivo, posta elettronica, raccomandata, istanza

di accesso ex L. 241/90), il ricevente provvede tempestivamente ad inoltrare la suddetta richiesta al DPO, mettendo in copia conoscenza il Responsabile e il Coordinatore.

Il Responsabile Privacy, con il supporto del Coordinatore Privacy, e del DPO ha la responsabilità di prendere in carico la richiesta, di procedere all'istruttoria e alla conseguente valutazione ai fini del tempestivo riscontro all'Interessato affinché le tempistiche di risposta siano in linea con i termini previsti dal Regolamento[1].

Qualora la richiesta non risulti sufficientemente chiara ed esaustiva, il Responsabile Privacy può inoltrare per compilazione all'Interessato il modulo previsto dall'Allegato 1 del presente documento, al fine di rendere maggiormente esplicito il contenuto della stessa.

4.3 Valutazione della richiesta

Il Responsabile Privacy, di concerto con il Coordinatore Privacy, coinvolgendo e coordinando il DPO e gli uffici di pertinenza, effettua una valutazione sulla fondatezza della richiesta pervenuta e, se del caso, verifica l'identità dell'Interessato richiedendone un documento di riconoscimento.

Il Responsabile Privacy, in considerazione delle indicazioni ricevute dai suddetti soggetti coinvolti, può rifiutare di soddisfare la richiesta dell'Interessato dando evidenza allo stesso mediante indicazione degli elementi che dimostrino il carattere manifestamente infondato o eccessivo della richiesta medesima.

Qualora la richiesta sia fondata, il Responsabile Privacy, di concerto con il Coordinatore Privacy, esegue le attività necessarie per l'evasione della richiesta (ad esempio identificazione dei dati all'interno dei sistemi gestionali in uso o negli archivi presso gli uffici e modifica e/o cancellazione degli stessi sui sistemi/archivi).

4.4 Invio della risposta all'Interessato

Il riscontro all'Interessato deve essere fornito in forma concisa, trasparente ed intellegibile, e deve essere realizzata con linguaggio semplice e chiaro.

[1] Art. 12 del GDPR "senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Il titolare del trattamento informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta."

Tenuto conto delle operazioni eseguite e delle informazioni raccolte, la risposta è predisposta dal Responsabile Privacy, con il supporto del Coordinatore Privacy e del DPO, mediante la compilazione del Modulo di Risposta di cui all'Allegato 2 del presente documento, sottoscritta e approvata dal Titolare.

4.5 Modalità di archiviazione

Il Titolare del trattamento, sempre per il tramite del Responsabile Privacy, è tenuto a registrare l'istanza ricevuta nel Registro delle Istanze degli Interessati, che contiene le seguenti informazioni minime:

- Soggetto registrante;
- Data ricezione dell'istanza;
- Nome e cognome dell'Interessato;
- Tipo di diritto esercitato;
- Data di invio risposta all'Interessato;
- Soggetti terzi coinvolti;
- Note.

Per la tenuta del registro vengono adottate idonee misure atte a garantire l'integrità e l'immodificabilità delle registrazioni, mediante salvataggio in una cartella con accesso limitato alle sole persone autorizzate;

Il Comune di Porto Azzurro archivia la documentazione cartacea ed elettronica relativa all'istanza presso la propria Segreteria.

Le cartelle elettroniche sono soggette a back up.

I faldoni cartacei sono archiviati in armadi chiusi a chiave presso la sede del Comune.

5. APPLICAZIONE DEI PRINCIPI DI PRIVACY BY DESIGN E PRIVACY BY DEFAULT

5.1 Premessa

Ogni qualvolta sia previsto lo sviluppo di un nuovo processo/servizio/attività/iniziativa/strumento che comporta il trattamento di dati personali di cui il Comune ne è Titolare o la modifica (di scopo o delle modalità) di un trattamento di dati personali già esistente, il Responsabile dell'Ufficio interessato dal suddetto sviluppo o

modifica, con il supporto degli incaricati al trattamento del proprio Ufficio, coinvolge il DPO, già in fase di progettazione del suddetto processo / servizio / attività / iniziativa / strumento e, ove necessario, il Responsabile della Transizione Digitale.

5.2 Modalità operativa

In tale contesto il Responsabile Privacy e gli incaricati presso il proprio Ufficio, con la collaborazione del DPO:

- predispongono una descrizione della soluzione TO BE relativa al nuovo processo/servizio/attività/iniziativa/strumento che si intende porre in essere;
- individuano i dati personali che saranno oggetto di trattamento, prevedendo che siano quelli minimi necessari al perseguimento delle finalità individuate in coerenza con il principio di minimizzazione dei dati;
- individuano le operazioni di trattamento che saranno svolte sui dati (tra cui 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), fornendo, ove necessario, indicazioni in merito alla limitazione della raccolta dei dati, con l'obiettivo di limitare i trattamenti a quelli strettamente necessari per la realizzazione delle finalità perseguite;
- individuano la finalità/le finalità per la quale/le quali si effettuerà il trattamento dei dati personali;
- individuano, anche con il supporto del Responsabile esterno del trattamento per la gestione dei sistemi informatici, le misure di sicurezza che si prevede di porre in essere (o che sono già poste in essere) a tutela dei dati personali oggetto del trattamento;
- individuano i dipendenti e/o collaboratori e/o altri soggetti terzi che, per lo svolgimento delle rispettive mansioni, avranno accesso ai dati personali, al fine di provvedere, qualora opportuno, alla formalizzazione di appositi documenti quali a titolo esemplificativo, istruzioni per il trattamento, protocolli di intesa o nomina in qualità di Responsabile esterno del trattamento, a seconda del caso;

- qualora le nuove attività comportino un nuovo trattamento sui dati personali precedentemente non censito o una modifica di un trattamento già esistente sul "Registro delle attività di trattamento", predispongono, con il supporto degli incaricati coinvolti nello sviluppo del processo/servizio/attività/iniziativa/strumento, una prima versione provvisoria del nuovo trattamento, così da censirlo, successivamente, sul Registro dei trattamenti; qualora le nuove attività comportino una modifica ad un trattamento già censito sul Registro dei trattamenti, predispongono una proposta di modifica al trattamento;
- eseguono le attività di Data Protection Impact Assessment (DPIA) per valutare se il nuovo trattamento, o il trattamento oggetto di modifica, possa presentare un rischio elevato per i diritti e le libertà degli Interessati;
- con la collaborazione del DPO, definiscono il periodo di conservazione dei dati (tale periodo può essere determinato sulla base della durata del trattamento previsto, sulla base delle finalità per le quali si intende eseguire il trattamento, nonché tenendo conto di eventuali obblighi imposti da norme vigenti);
- in funzione delle informazioni ricevute in merito all'eventuale trasferimento di dati in Paesi extra UE (compreso UK), verificano ed evidenziano:
    - se il Paese verso cui sono trasferiti i dati garantisce un livello di protezione dei dati adeguato a quello europeo, laddove tale livello di protezione sia confermato dalla Commissione Europea mediante "Decisione di adeguatezza";
    - che il trasferimento non ricada in una delle condizioni previste dall'art. 49 del GDPR;

  Nel caso in cui non sia presente nessuna delle condizioni su riportate, il DPO verifica, qualora richiesto dagli incaricati dell'Ufficio interessato, le soluzioni proposte / adottate dagli stessi per la regolamentazione del trattamento in modo da risultare conforme alla normativa in materia di protezione dei dati personali, come la predisposizione di accordi contrattuali ad hoc con la terza parte (in questo caso gli accordi dovranno prevedere l'indicazione puntuale delle misure di sicurezza poste in essere dalla terza parte, che dovranno essere valutate dal Comune), la

predisposizione di clausole contrattuali Standard adottate dalla UE, la richiesta di consenso specifico all'Interessato; il DPO verifica, se richiesto dal Titolare per il tramite degli incaricati dell'Ufficio interessato, l'attendibilità dei risultati della DPIA;

- ove necessario, richiedono al DPO la validazione della DPIA e se del caso un parere scritto in merito alle evidenze emerse dalla sua analisi/valutazione, in particolare riguardo:
    - alla correttezza in merito al rispetto del principio di minimizzazione dei dati;
    - alla definizione delle tempistiche di conservazione dei dati;
    - ai risultati della DPIA, quindi in merito all'effettiva adeguatezza delle misure di sicurezza poste in essere o che si prevede di porre in essere a garanzia della protezione dei dati;
    - alla verifica delle dovute informative privacy verso gli Interessati, con l'indicazione della necessità di richiedere consensi specifici agli Interessati;
    - qualora lo ritenga necessario, informa il Titolare del trattamento in merito ai risultati delle sue analisi/valutazioni;

  ricevuto il feedback da parte del DPO, qualora decidessero di accogliere tale parere, indirizzano le attività in funzione di quanto indicato dallo stesso, coinvolgendo i Responsabili degli Uffici coinvolti dal trattamento o comunicando al Responsabile esterno del trattamento per la gestione dei sistemi informatici l'eventuale necessità di predisporre:
    - soluzioni tecnologiche rivolte alla cancellazione o alla pseudonimizzazione o alla crittografia dei dati, da applicare ai dati personali oggetto del trattamento allo scadere delle tempistiche di conservazione identificate;
    - l'implementazione di ulteriori misure di sicurezza da implementare al fine di ridurre il rischio residuo fino a portarlo ad un livello di tolleranza accettabile, nel caso in cui dalla DPIA si evidenzi un rischio residuo "Alto" per le libertà e i diritti degli Interessati.

In considerazione delle nuove misure di sicurezza individuate e da implementare, gli incaricati dell'Ufficio interessato eseguono una nuova DPIA, effettuando una simulazione sull'ipotesi delle suddette nuove misure di sicurezza, fornendo al DPO le evidenze emerse. In questo caso:

- se i risultati dalla nuova DPIA indicano che, con l'implementazione delle nuove misure di sicurezza previste/ipotizzate, il rischio residuo si riduce fino ad un livello di tolleranza accettabile, gli incaricati dell'Ufficio interessato, previo parere del DPO, indirizzano i Responsabili degli Uffici coinvolti dal trattamento o il Responsabile esterno del trattamento per la gestione dei sistemi informatici per l'implementazione delle nuove misure di sicurezza (in questo caso la realizzazione del nuovo processo / servizio / attività / iniziativa / strumento è vincolato all'implementazione delle nuove misure di sicurezza);
- se i risultati dalla nuova DPIA indicano che, con l'implementazione delle nuove misure di sicurezza previste/ipotizzate, il rischio residuo non si riduce fino ad un livello di tolleranza accettabile gli incaricati dell'Ufficio interessato coinvolgono il DPO per l'esecuzione delle attività necessarie ad indirizzare il parere al Garante per la protezione dei dati personali, prima di procedere al trattamento.

In tale contesto, ai sensi dell'articolo 36 del GDPR, il DPO richiede, per conto del Titolare, la consultazione preventiva al Garante per la protezione dei dati personali, comunicando:

- le responsabilità del Titolare ed eventualmente quelle dei Contitolari o Responsabili esterni del trattamento;
- le finalità e i mezzi del trattamento previsto;
- le misure e le garanzie previste per proteggere i diritti e le libertà degli Interessati;
- i dati di contatto del Titolare e del DPO;
- la valutazione di impatto sulla protezione dei dati effettuata;
- ogni altra informazione richiesta dall'autorità competente.

Il Garante per la protezione dei dati personali fornisce entro un termine di otto settimane (termine che può essere prorogato di ulteriori sei settimane) un parere scritto al Titolare del trattamento. In seguito alla ricezione del feedback da parte dell'Autorità, e alla condivisione dello stesso con il DPO e con gli incaricati dell'Ufficio interessato, questi ultimo, con il supporto del DPO, verificano l'opportunità di poter procedere all'implementazione del nuovo processo/servizio/attività/iniziativa/strumento secondo le indicazioni fornitore dall'Autorità.

Nel caso in cui si possa procedere con lo sviluppo del nuovo processo/servizio/attività/iniziativa/strumento o la modifica (di scopo o delle modalità) di un trattamento di dati personali già esistente, gli incaricati dell'Ufficio interessato:

- monitorano lo svolgimento delle attività relative alla realizzazione processo / servizio / attività / iniziativa / strumento, accertandosi dell'effettiva implementazione/adozione delle misure di sicurezza previste a garanzia della protezione dei dati e del rilascio dei documenti da predisporre in conformità con la normativa vigente in materia di protezione dei dati personali (ad es. informative privacy, aggiornamento registro dei trattamenti);
- in un momento precedente al rilascio del nuovo processo/servizio/attività/iniziativa/strumento, effettuano, insieme ai Responsabili degli Uffici coinvolti nel trattamento e, ove necessario, al Responsabile esterno del trattamento per la gestione dei sistemi informatici, dei test e/o verifiche sulla corretta applicazione dei principi privacy ai sensi dell'articolo 5 del GDPR e implementazione delle misure di sicurezza per la protezione dei dati, comunicando i risultati degli stessi al DPO; in caso di esiti negativi, gli incaricati dell'Ufficio interessato effettueranno i dovuti adeguamenti al fine di ottenere riscontri positivi.

Nota: nel caso in cui gli incaricati dell'Ufficio interessato, in accordo con il Titolare, non dovessero accogliere il parere del DPO sulla DPIA, gli stessi documenteranno, attraverso apposito verbale, le motivazioni che li hanno indotti a non accogliere il parere.

5.3 Modalità di archiviazione

Il Titolare del trattamento, sempre per il tramite del Responsabile Privacy, archiviano la documentazione relativa ai controlli effettuati e la relazione contenente gli esiti della valutazione finale, all'interno della cartella di rete predisposta. Deve essere prevista la creazione di una sottocartella apposita per ciascun processo/servizio/attività/iniziativa/ strumento oggetto di valutazione.

6. GESTIONE E NOTIFICA DEL DATA BREACH

6.1 Premessa

Data breach è 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." Tale violazione può riguardare:

- "la riservatezza dei dati personali", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;
- "l'integrità dei dati personali", in caso di modifica non autorizzata o accidentale dei dati personali;
- "la disponibilità dei dati personali", in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.

Una singola violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse.

La tabella successiva, a titolo esemplificativo, riporta alcuni eventi che possono implicare un data breach, qualora siano coinvolti dati personali:

a. Perdita o furto di dispositivi del Comune;
b. Perdita o furto di supporti mobili quali pen-drive USB o hard disk del Comune;
c. Perdita o furto di fascicoli cartacei o altra documentazione del Comune;
d. Phishing (es. installazione di software non autorizzata, ricezione di una mail con mittente avente dominio sconosciuto, apertura di allegati a mail che nascondono ransomware o malware);
e. Invio erroneo di comunicazioni/informazioni verso l'esterno (es. errato inserimento del destinatario in una comunicazione da parte del Comune ovvero errato invio ad un destinatario differente rispetto a quello inserito nella predisposizione della mail);
f. Alterazione non autorizzata o impropria dei dati personali (es. mancata protezione dei personal computer del Comune);
g. Impossibilità di trattare i dati personali per cause accidentali o per interruzione dei sistemi (es. distruzione accidentale di un documento ovvero interruzione dei sistemi per calamità naturali, virus o attacco cyber);

h. Situazioni anomale segnalate o riscontrate nei sistemi informatici (es. rilevazione da parte dei sistemi informatici di infezione da virus, malware, ransomware);
i. Divulgazione non autorizzata dei dati personali (es. comunicazione o diffusione non sicura o illecita, anche attraverso i media, di dati personali, di cui il Comune ne è Titolare o Responsabile o comportamenti sleali o fraudolenti di dipendenti).

6.2 Segnalazione del data breach

La rilevazione di un potenziale evento data breach può derivare da:

- la segnalazione di un dipendente, un cliente, un ospite, un fornitore, un collaboratore, un consulente;
- la segnalazione da parte del Responsabile esterno del trattamento, tra cui la società che si occupa della gestione dei sistemi informatici;
- la comunicazione da parte delle Forze di Polizia o da altre Autorità;
- l'alert automatico dei sistemi informatici.

Le segnalazioni devono avvenire in relazioni ad eventi per cui è presente:

- coinvolgimento in prima persona;
- osservazione diretta;
- possesso o presa visione di evidenze documentali;
- divulgazione di notizie da parte dei media;

In caso di un potenziale evento data breach, si deve riferire senza alcun indugio o ritardo al DPO, al Responsabile delegato Privacy e al Coordinatore Privacy. Quest'ultimo, o il Responsabile Privacy in caso di assenza del coordinatore, provvede alla gestione e valutazione del potenziale data breach, compilando il modulo di cui all'allegato 3 del presente documento, con il supporto del Responsabile Privacy, del DPO, degli incaricati dell'Ufficio che sono impattati dal potenziale evento data breach e, ove necessario, del Responsabile esterno del trattamento / specialisti esterni.

6.3 Gestione del data breach

Il Coordinatore Privacy, con il supporto del DPO, effettua tempestivamente una prima analisi della segnalazione per identificare con ragionevole certezza la presenza del data breach e per valutarne l'impatto sulla protezione dei dati personali.

Il Coordinatore Privacy, supportato dal Responsabile Privacy, può effettuare indagini di approfondimento con lo scopo di raccogliere evidenze e altre informazioni pertinenti presso gli Uffici del Comune impattati dal potenziale evento data breach, avvalendosi del supporto di specialisti esterni e/o di altri Uffici del Comune e/o Responsabili esterni del trattamento.

Tutti i soggetti coinvolti devono garantire la riservatezza delle informazioni comunicate o rilevate durante la gestione del data breach.

Il data breach deve essere valutato con riferimento all'impatto sui diritti e alle libertà degli Interessati. Tale impatto rileva in termini di danno alle persone fisiche:

- fisico (es. rischio di frode o usurpazione d'identità che comportano in caso di persona vulnerabile un danno fisico);
- materiale (es. perdite finanziarie);
- immateriale (es. pregiudizio alla reputazione).

Al fine di stimare l'entità dell'impatto si considerano complessivamente i seguenti aspetti:

a. il tipo di violazione;
b. la natura del dato personale violato;
c. il volume dei dati personali violati in termine di tempo e contenuto;
d. la facilità di identificazione delle persone fisiche interessate;
e. la gravità delle conseguenze;
f. le caratteristiche particolari degli Interessati coinvolti;
g. il numero delle persone fisiche coinvolte.

La valutazione del rischio connesso al data breach viene eseguita in considerazione delle metodologie riconosciute dal Garante per la protezione dei dati personali o dalle best practice in materia (ad esempio, ENISA).

La valutazione del data breach è formalizzata secondo il modello di cui all'allegato 4 del presente documento, sottoscritto dal Titolare del trattamento.

Il Coordinatore Privacy, insieme al DPO e al Responsabile Privacy, ed eventualmente al Responsabile esterno del trattamento / specialisti esterni, individuano la strategia di gestione dell'evento, anche al fine di minimizzare l'eventuale danno.

Qualora l'evento fosse ancora in corso, è opportuno definire:

a. le modalità di contenimento attraverso misure tecniche ed organizzative di protezione (ad esempio, denuncia di smarrimento, blocco da remoto dei dispositivi, recupero dei dati tramite back up, isolamento delle utenze, reset delle password);
b. le modalità di monitoraggio della situazione (ad esempio, analisi e monitoraggio dei log, del traffico di rete e funzionamento del firewall);
c. eventuale piano delle comunicazioni interne ed esterne (ad esempio, predisposizione di una comunicazione interna dell'accaduto oppure di una comunicazione da rendere pubblica attraverso media, Forze dell'Ordine, sito istituzionale);
d. a seguito della ricostruzione dell'accaduto, le azioni correttive per contenere i danni, rispristinare l'accesso ai dati e assicurare la resilienza dei sistemi (ad esempio, denuncia di smarrimento, blocco da remoto dei dispositivi, recupero dei dati tramite back up, isolamento delle utenze, reset delle password).

Qualora l'evento fosse già avvenuto, è opportuno definire i punti c) e d) del punto elenco di cui sopra.

Le misure correttive individuate e riportate all'interno del documento di valutazione del data breach sono comunicate ai Responsabili degli Uffici con il supporto, ove necessario, dei Responsabili esterni del trattamento, che le devono implementare.

Il Coordinatore Privacy con il supporto del DPO monitora la completa e corretta attuazione delle misure, in considerazione delle scadenze previste, riferendo al Titolare del trattamento.

6.4 Modalità di notifica al Garante per la protezione dei dati personali

Nel caso in cui il data breach abbia effetti avversi significativi sui diritti e le libertà degli Interessati, causando danni fisici, materiali o immateriali, si procede obbligatoriamente alla notifica nei confronti del Garante per la protezione dei dati personali ovvero anche alla comunicazione agli Interessati coinvolti dalla violazione.

Il Coordinatore Privacy, con il supporto del DPO e del Responsabile Privacy, predispone la notifica da far sottoscrivere al Titolare, o suoi delegati, così da inviarla al Garante per la protezione dei dati personali, come indicato nel link dell'Autorità stessa, secondo il modello di "notifica di una violazione dei dati personali.

La notifica viene inoltrata senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui il Titolare del trattamento, o suoi delegati, ne è venuto a conoscenza ossia nel momento in cui è ragionevolmente certo che si è verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali. Oltre tale termine, la notifica deve essere corredata delle ragioni del ritardo.

Qualora non sia possibile fornire tutte le informazioni contestualmente alla notifica, queste ultime potranno essere fornite in fasi successive senza ulteriore ingiustificato ritardo, avendo cura di dare evidenza delle motivazioni per cui tali informazioni non siano disponibili all'interno della notifica.

Nel caso in cui sia il Garante per la protezione dei dati personali ad ordinare con provvedimento l'applicazione di ulteriori misure correttive rispetto alla violazione notificata, sarà cura del DPO supervisionare sulla completa e corretta implementazione delle suddette misure.

6.5 Comunicazione della violazione agli Interessati

Qualora non siano state predisposte o adottate misure adeguate al rischio o il data breach comporti un rischio elevato per gli Interessati, il Coordinatore Privacy, con il supporto del DPO e del Responsabile Privacy, invia, senza ingiustificato ritardo, la comunicazione ai suddetti sottoscritta dal Titolare del trattamento o suoi delegati.

La comunicazione deve essere predisposta con un linguaggio semplice e chiaro, secondo il modello di cui all'allegato 5 del presente documento.

La modalità di comunicazione dovrà tenere in considerazione, ove necessario, delle diversità linguistiche dei destinatari.

Nel caso in cui sia il Garante per la protezione dei dati personali ad ordinare con provvedimento la comunicazione del data breach agli Interessati, il Titolare del trattamento, o suoi delegati, provvede alla stessa.

6.6 Modalità di archiviazione

Il Titolare del trattamento, sempre per il tramite del Coordinatore Privacy, registra tutte le segnalazioni pervenute all'interno del Registro Interno delle Violazioni, indipendentemente dalle notifiche che saranno effettuate a seguito della valutazione del data breach.

Il suddetto registro ha la funzione di documentare le valutazioni effettuate e le decisioni prese per porre rimedio alle violazioni avvenute.

In particolare, il Registro contiene le seguenti informazioni minime:

- Ufficio interessato dall'evento;
- Soggetto segnalante;
- Data segnalazione;
- Data evento;
- Dati interessati;
- Interessati;
- Classificazione dell'evento (in termini di Confidenzialità, Integrità, Disponibilità);
- Eventuale Notifica all'Autorità e data di invio;
- Eventuale comunicazione agli Interessati coinvolti e data di invio;
- Remedies.

Per la tenuta del registro vengono adottate idonee misure atte a garantire l'integrità e l'immodificabilità delle registrazioni in esso contenute, quali:

- Salvataggio in una cartella con accesso limitato alle sole persone autorizzate;
- Protezione delle celle per evitare che i dati siano modificati da persone non autorizzate;
- Salvataggio con password di sola lettura in modo che il documento non possa essere modificato da persone non autorizzate.

Il Titolare del trattamento, sempre per il tramite del Coordinatore Privacy, archivia la documentazione cartacea ed elettronica emersa in sede di segnalazione e valutazione del data breach, nonché della documentazione relativa alle notifiche trasmesse al Garante per la protezione dei dati personali e alle comunicazioni nei confronti degli Interessati presso la propria Segreteria.

Le cartelle elettroniche sono soggette a back up.

I faldoni cartacei sono archiviati in armadi chiusi a chiave presso la sede del Comune.

7. MODALITÀ DI GESTIONE DELLE TERZE PARTI

Nel caso in cui sia in corso la contrattualizzazione di un fornitore, per indirizzare le attività di "gestione" della terza parte in maniera *compliant* alla normativa in materia di protezione dei dati personali, è opportuno, già in fase contrattuale/precontrattuale:

- sapere se il fornitore, nell'ambito dell'erogazione dei propri servizi verso il Comune, effettuerà un trattamento dei dati personali di cui il Comune di Porto Azzurro è Titolare;
- essere a conoscenza di eventuali sub-fornitori cui il fornitore intende rivolgersi per affidare in tutto o in parte le attività che comportano l'erogazione dei servizi verso il Comune e se tali sub-fornitori potranno effettuare, nell'esecuzione delle attività affidategli, trattamenti su dati personali di cui il Comune è Titolare;
- essere a conoscenza dell'ubicazione geografica di server/DB, del fornitore e/o dei subfornitori, su cui possono risiedere o su sui possono transitare anche temporaneamente dati personali di cui il Comune è Titolare.

Il Responsabile dell'Ufficio, che detiene i rapporti con il fornitore, può far sottoporre al fornitore il questionario, di cui all'Allegato 6 del presente documento, al fine di rilevare le informazioni utili ad indirizzare, già in fase contrattuale/pre-contrattuale, le attività relative a:

- l'eventuale iter di designazione del fornitore come Responsabile esterno del trattamento dei dati personali;
- la valutazione delle misure di sicurezza proposte, ove necessario;
- l'indirizzamento delle attività per regolamentare, in modo che risulti compliant a quanto previsto dalla normativa in materia di protezione dei dati personali, l'eventuale trasferimento di dati in Paesi extra UE.

8. DEFINIZIONI

Dato personale *(ai sensi dell'art. 4. n. 1, del GDPR): "qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale".*

Interessato *(ai sensi dell'art. 4, n. 1, del GDPR): "la persona fisica identificata o identificabile. L'interessato si identifica in colui che ha conferito i propri dati personali al Titolare del trattamento"*

Trattamento *(ai sensi dell'art. 4. n. 2, del GDPR): "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."*

Limitazione di trattamento *(ai sensi dell'art. 4, n. 3, del GDPR): "il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro";*

Profilazione *(ai sensi dell'art. 4, n. 3, del GDPR): "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";*

Archivio *(ai sensi dell'art. 4, n. 6, del GDPR): "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."*

Titolare del trattamento *(ai sensi dell'art. 4. n. 7, del GDPR): "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."*

Contitolari del trattamento *(ai sensi dell'art. 26 del GDPR): "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, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14 del GDPR, 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. L'accordo di cui al paragrafo precedente 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 di cui al paragrafo precedente, l'interessato può esercitare i propri diritti ai sensi del Regolamento nei confronti di e contro ciascun titolare del trattamento."

Responsabile del trattamento *(ai sensi dell'art. 4. n. 8, del GDPR): "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento."*

Consenso dell'interessato *(ai sensi dell'art. 4. n. 11, del GDPR): "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";*

Incaricato *(ai sensi dell'articolo 29 del GDPR)**:** soggetto che agisce sotto l'autorità e secondo le istruzioni impartite del Titolare del trattamento, che ha accesso ai dati personali nell'ambito e per lo svolgimento delle sue attività.*

Responsabile per la Protezione dei Dati Personali *(c.d. Data Protection Officer o DPO): la persona fisica individuata dal Comune di Porto Azzurro. Ai sensi dell'articolo 39 del GDPR, il DPO ha il compito di:*

- *informare e fornire consulenza al Titolare del trattamento, nonché ai dipendenti che eseguono il trattamento, in merito agli obblighi derivanti dal GDPR e dalle altre disposizioni dell'Unione Europea o delle normative nazionali degli Stati membri relative alla protezione dei Dati;*
- *sorvegliare l'osservanza del regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare del trattamento o del Responsabile 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;*
- *fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;*
- *cooperare con il Garante per la protezione dei dati personali;*
- *fungere da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.*

Diritto di Accesso ai Dati *(ai sensi dell'art. 15 del Regolamento): L'interessato ha diritto di ottenere dal titolare 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:*

- le finalità del trattamento;

- le categorie di dati personali in questione;

- 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;

- quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

- 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;

- il diritto di proporre reclamo a un'autorità di controllo;

- qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;

- l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, 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'articolo 46 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.

***Diritto di Rettifica**: (ai sensi dell'art. 16 del Regolamento): 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.*

***Diritto alla Cancellazione** ("diritto all'oblio"): (ai sensi dell'art. 17 del Regolamento): L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:*

- *i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;*
- *l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;*
- *l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;*
- *i dati personali sono stati trattati illecitamente;*
- *i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;*
- *i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.*

Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:

- *per l'esercizio del diritto alla libertà di espressione e di informazione;*
- *per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;*
- *per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;*
- *a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;*
- *o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.*

***Diritto di Limitazione al trattamento** (ai sensi dell'art. 18 del Regolamento): L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:*

- *l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;*
- *il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;*
- *benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;*
- *l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.*

Se il trattamento è limitato a norma del paragrafo 1, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

L'interessato che ha ottenuto la limitazione del trattamento a norma del paragrafo 1 è informato dal titolare del trattamento prima che detta limitazione sia revocata. impossibilità di trattamento del dato da parte del titolare in caso di richiesta rettifica o di opposizione al trattamento da parte dell'interessato.

***Diritto alla Portabilità dei dati** (ai sensi dell'art. 20 del Regolamento): L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:*

- *il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e*
- *il trattamento sia effettuato con mezzi automatizzati.*

Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.

L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17. Tale diritto non si applica al trattamento 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.

Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui.

***Diritto di Opposizione** (ai sensi dell'art. 21 del Regolamento): 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), 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.*

Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.

Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità.

Il diritto di cui ai paragrafi 1 e 2 è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.

Nel contesto dell'utilizzo di servizi della società dell'informazione e fatta salva la direttiva 2002/58/CE, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.

Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

***Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione** (ai sensi dell'art. 22 del Regolamento): 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.*

Il paragrafo 1 non si applica nel caso in cui la decisione:

a) *sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;*
b) *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 e dei legittimi interessi dell'interessato;*
c) *si basi sul consenso esplicito dell'interessato.*

Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione *(ai sensi dell'art. 25 del Regolamento): Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.*

Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

Privacy by Design *(ai sensi dell'art. 25 del Regolamento): 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*

Privacy by Default *(ai sensi dell'art. 25 del Regolamento): Necessità di configurare il trattamento prevedendo cha solo i dati personali necessari per ogni specifica finalità del trattamento siano trattati, per impostazione predefinita. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità.*

Distruzione dei dati personali *(ai sensi delle Linee guida sulla notifica delle violazioni dei dati personali ai sensi del GDPR del Gruppo di lavoro "Articolo 29"): "i dati personali non esistono più o non esistono più in una forma che sia di qualche utilità per il Titolare del trattamento."*

Data Breach *(ai sensi dell'art. 4. n. 12, del GDPR): "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."*

Ai sensi delle Linee guida sulla notifica delle violazioni dei dati personali ai sensi del GDPR del Gruppo di lavoro "Articolo 29", la violazione dei dati personali può essere classificata come segue:

- "violazione della riservatezza", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;

- "violazione dell'integrità", in caso di modifica non autorizzata o accidentale dei dati personali;

- "violazione della disponibilità", in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.

Una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse.

Danno *(ai sensi delle Linee guida sulla notifica delle violazioni dei dati personali ai sensi del GDPR del Gruppo di lavoro "Articolo 29"): "i dati personali sono stati modificati, corrotti o non sono più completi."*

Perdita dei dati personali *(ai sensi delle Linee guida sulla notifica delle violazioni dei dati personali ai sensi del GDPR del Gruppo di lavoro "Articolo 29"): "i dati potrebbero comunque esistere, ma il Titolare del trattamento potrebbe averne perso il controllo o l'accesso, oppure non averli più in possesso. Un esempio di perdita di dati personali può essere la perdita o il furto di un dispositivo contenente una copia della banca dati dei clienti del Titolare del*

trattamento, o il caso in cui l'unica copia di un insieme di dati personali sia stata crittografata da un ransomware (malware del riscatto) oppure dal Titolare del trattamento mediante una chiave non più in suo possesso."

Trattamento non autorizzato o illecito *(ai sensi delle Linee guida sulla notifica delle violazioni dei dati personali ai sensi del GDPR del Gruppo di lavoro "Articolo 29"): "può includere la divulgazione di dati personali a (o l'accesso da parte di) destinatari non autorizzati a ricevere (o ad accedere a) i dati oppure qualsiasi altra forma di trattamento in violazione del regolamento."*