POLICY AZIENDALE RELATIVA ALLA GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI

Premesse

La presente Policy è stata redatta nel rispetto del Regolamento europeo per la protezione dei dati personali n. 2016/679 (di seguito "**GDPR**") e delle "*Guidelines on Personal data breach notification under Regulation 2016/679"* pubblicate dal gruppo di lavoro *Article 29 Data Protection Working Party*.

La presente procedura ("Procedura") viene redatta per assicurare la risposta più adeguata ad una violazione di dati personali degli interessati trattati dalla Società Extetica Group S.r.l. come Titolare o come Responsabile del trattamento.

In particolare, gli obiettivi del presente documento sono:

- Creare un piano di gestione e risposta in caso di violazione di dati;
- Definire i criteri di valutazione della gravità dei rischi per gli interessati;
- Definire un processo di notifica all'autorità di vigilanza competente e (se del caso) agli interessati.

La Policy si applica ed è rivolta a tutti i dipendenti e collaboratori della Società.

1. Definizioni

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali.

Dato personale: qualsiasi informazione riguardante una persona fisica che sia identificata o comunque identificabile (ad esempio, dati anagrafici, numeri di telefono, indirizzi e-mail, indirizzo IP, numero di carta di credito).

Categorie particolari di dati personali: dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni filosofiche, o l'appartenenza sindacale, nonché dati sanitari, genetici, biometrici, relativi alla vita sessuale o all'orientamento sessuale di una persona.

Interessato: Persona fisica identificata o identificabile cui si riferiscono i dati personali.

Titolare del trattamento: 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.

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.

Responsabile della protezione dei dati (DPO): il *Data Protection Officer* è nominato dal titolare del trattamento e dal responsabile del trattamento secondo le prescrizioni di cui alla sezione 4 del Capo IV del GDPR

Referente di Area: figura di riferimento di ogni dipartimento e/o ufficio.

Referente Privacy: referente incaricato di assistere la Società, a livello locale, ai fini dell'adeguamento al GDPR ed ai fini dell'osservanza di tutte le normative vigenti in materia di privacy e di protezione dei dati personali

2. Ambito di applicazione

2.1 Violazione di dati personali

Ai sensi dell'art. 4, par. 1, n. 12 del GDPR, per violazione di dati si intende "*la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".*

I dati violati possono includere qualsiasi tipologia di Dati Personali, dai dati c.d. ordinari (come ad esempio, dati anagrafici, numeri di telefono, indirizzi e-mail), a Categorie Particolari di Dati Personali (o dati sensibili, come ad esempio, dati sanitari, dati religiosi o relativi ad un'appartenenza sindacale).

Le violazioni di dati possono essere classificate secondo i tre seguenti principi di sicurezza delle informazioni:

Violazione di riservatezza: quando vi è un accesso o una divulgazione non autorizzata o accidentale di Dati Personali;

Violazione dell'integrità: quando vi è una modifica o un'alterazione non autorizzata o accidentale di Dati Personali;

Violazione della disponibilità: quando si verifica una distruzione di Dati Personali o di perdita di disponibilità accidentale o non autorizzata di Dati Personali.

2.2. Cause

Una violazione di Dati Personali potrebbe essere provocata da diversi eventi, ad esempio, da un dipendente o da un soggetto esterno alla società (quale conseguenza di un errore umano o di un'attività fraudolenta) o da un mal funzionamento di un sistema informatico.

A. Esempi di **errore umano** posso essere:
    i. Smarrimento di una risorsa informatica della società (un personal computer o un tablet) contenente dati personali;
    ii. Comunicazione di Dati Personali a un destinatario non corretto;
    iii. Utilizzo di un data base contenente Dati Personali in un modo non corretto o non autorizzato (ad esempio, effettuando una copia personale di dati);
    iv. Smaltimento improprio di una risorsa informatica contenente Dati Personali (ad esempio, lo smaltimento di un hard disk o di un personal computer in discarica prima di aver cancellato e/o distrutto tutti i documenti archiviati).

B. Esempi di **attività fraudolente** posso essere:
    i. Attività di *hacking* (ad esempio, un accesso illegale ad un database contenente Dati Personali);
    ii. Furto di una risorsa informatica della società (un personal computer, tablet) contenenti Dati Personali;
    iii. Truffe informatiche da cui segue una diffusione non autorizzata di Dati Personali.

C. Esempi di **malfunzionamento di un sistema informatico** possono essere:
    i. Errore/bug in un software della società, tale da determinare una perdita di disponibilità di Dati Personali;
    ii. Guasti a sistemi di *cloud computing* o *cloud storage*;
    iii. Perdita di chiavi di accesso a database.

Come si specificherà in seguito, qualora si verifichi una o più delle suindicate violazioni, vige per il Titolare del trattamento un obbligo di notifica all'autorità di vigilanza (in caso di rischio per i diritti e le libertà delle persone coinvolte, art. 33 GDPR) e, se del caso, agli interessati (in caso di rischio elevato per i diritti e le libertà delle persone coinvolte, art. 34 GDPR).

3. Piano di risposta in caso di violazione di dati

La Società ha adottato misure di sicurezza, tecniche ed organizzative, idonee a garantire un livello di protezione adeguato per i diritti e le libertà degli Interessati e, quindi, a prevenire possibili violazioni di dati personali.

Come parte integrante di tali misure di sicurezza, la Società ha anche implementato una procedura interna di risposta ad eventuali violazioni di Dati Personali, al fine di rilevare e gestire tali violazioni.

Chiunque venga a conoscenza di un possibile incidente che possa comportare una violazione di Dati Personali dovrà, infatti, riportare immediatamente l'accaduto al proprio Referente di Area, che provvederà ad inoltrare la richiesta al Referente Privacy.

Il Referente Privacy, con funzioni consultive e di controllo in materia di protezione dei dati personali, condividerà la segnalazione ricevuta con il DPO, che la valuterà attentamente al fine di procedere con l'attivazione del piano di gestione e risposta in caso di potenziali violazioni dei dati.

Resta, in ogni caso, inteso che tutti i dipendenti ed i collaboratori della Società, in special modo, ma non in senso limitativo tutti coloro che hanno accesso a Dati Personali, devono essere adeguatamente informati in merito ai contenuti della presente Policy.

4. Piano di gestione e risposta

Non appena sia pervenuta una segnalazione inerente una possibile violazione di Dati Personali, il Referente Privacy, su impulso del Referenti di Area – sentito anche il Responsabile per la Protezione dei Dati - deve immediatamente azionare il piano di gestione e risposta.

Il piano di gestione e risposta comprende:

A. Valutazione preliminare della segnalazione;

B. Valutazione e conferma di un'avvenuta violazione di Dati Personali.

C. Contenimento degli effetti della violazione.

D. Valutazione del rischio e dell'impatto sugli Interessati.

E. Notifica della violazione all'autorità di vigilanza e agli Interessati.

F. Comunicazione della violazione agli Interessati, per i casi di rischio elevato.

G. Documentazione dell'incidente nel registro delle violazioni.

5. Valutazione preliminare della segnalazione.

Non appena ricevuta una segnalazione, il Referente di Area ed il Referente Privacy procederanno ad un esame preliminare e sommario della stessa, al fine di valutarne i requisiti di attendibilità e serietà.

Non appena terminato tale esame sommario, che, in ogni caso, non potrà durare più di due ore, il Referente Privacy – a meno che la segnalazione non risulti essere palesemente priva di fondamento – provvederà ad inoltrare la segnalazione al Responsabile della Protezione dei Dati ("**DPO**").

6. Valutazione e conferma di un'avvenuta violazione di Dati Personali.

Il Referente Privacy, al fine di svolgere le necessarie attività d'indagine, deve prendere visione della segnalazione ed acquisire dai Referenti di Area e da tutti gli altri dipendenti e/o collaboratori della società, che a vario titolo possono essere coinvolti nella violazione, tutti gli elementi necessari ad accertare se vi sia stata o meno una reale violazione di Dati Personali.

7. Contenimento degli effetti della violazione.

Il Referente Privacy, sentito il DPO, avvisa il Titolare di porre in essere tutte le misure utili e/o necessarie per contenere il più possibile gli effetti della violazione, ad esempio:

i. Disabilitare il sistema compromesso che ha causato la violazione di dati;
ii. Stabilire se è possibile adottare misure per recuperare i dati persi e limitare i danni causati dalla violazione (es. disabilitando / cancellando da remoto un file contenente dati personali);
iii. Resettare le password e gli account compromessi.

8. Valutazione dei rischi per gli Interessati

Non tutti gli incidenti costituiscono una violazione di Dati Personali in grado di determinare un rischio per gli Interessati. Ad esempio, lo smarrimento di un personal computer contenente Dati Personali criptati non comporta alcun rischio per gli individui. In tal caso, come conseguenza, non sarà necessario procedere ad una notifica all'autorità di vigilanza. Se, invece, il personal computer contenesse anche le chiavi per decriptare i dati, potrebbe sussistere un rischio per i diritti e le libertà degli Interessati.

A tal fine, il Referente Privacy, anche con il supporto del DPO, sarà chiamato a considerare e documentare:

- Come e quando è avvenuta la violazione;
- Quali categorie di Dati Personali sono coinvolte nell'incidente (dati personali c.d. ordinari e/o categorie particolari di dati);
- A quante persone fanno riferimento i dati violati;
- A quali categorie di persone fanno riferimento i dati violati (dipendenti, clienti, fornitori, minori, ecc.);
- Quali sono i potenziali effetti e le conseguenze prodotte dalla violazione;
- Quali azioni sono state intraprese al fine di mitigare gli effetti della violazione.

Come già anticipato non tutte le violazioni di dati personali comportano un obbligo di notifica. Al fine di stabilire se una violazione determini automaticamente un obbligo di notifica all'autorità di vigilanza e/o agli Interessati, è necessario eseguire una valutazione del rischio e stabilire se la violazione costituisce un rischio per i diritti e le libertà dei soggetti coinvolti.

A tal proposito, il GDPR fa una distinzione tra:

- **Rischio**, la cui verificazione, ai sensi dell'art. 33 del GDPR, determina un obbligo di notifica all'autorità di vigilanza.
- **Rischio elevato**, la cui verificazione, ai sensi dell'art. 34 del GDPR, determina altresì un obbligo di notifica ai soggetti Interessati.

La violazione di dati può essere descritta come una violazione della riservatezza, dell'integrità o della disponibilità, o una combinazione di essi, idonea a causare al soggetto interessato un danno fisico, materiale o immateriale.

Esempi concreti di tali danni possono essere:

- Discriminazione,
- Furto di identità,
- Frode,
- Perdite finanziarie,
- Danno reputazionale.

A seconda delle circostanze, i danni alle persone coinvolte possono essere di diversa gravità. Ad esempio la violazione di un database contenente dati sanitari degli interessati deve essere sicuramente considerato come un rischio, anche elevato, per le persone coinvolte. Così come la violazione di dati di contatto per una newsletter, può comportare un rischio da cui potrebbe sorgere un obbligo di notifica all'autorità di vigilanza, ma non necessariamente un obbligo di comunicazione alle persone coinvolte.

9. Notificazione della violazione all'autorità di vigilanza

Ai sensi dell'art. 33 del GDPR, in caso di violazione di Dati Personali, il Titolare del trattamento deve notificare la violazione all'autorità di vigilanza senza ingiustificato ritardo e comunque entro 72 ore dal momento in cui ne sia venuto a conoscenza.

La notifica non è necessaria qualora appaia improbabile che la violazione di Dati Personali presenti un rischio per i diritti e le libertà per le persone coinvolte.

Di conseguenza, nel valutare il rischio per le persone a seguito di una violazione, il DPO dovrebbe considerare le circostanze specifiche della violazione, inclusa la gravità dell'impatto potenziale e la probabilità che tale rischio si concretizzi. Ai fini di tale valutazione, devono essere presi in considerazione i seguenti criteri:

- Il tipo di violazione (perdita di riservatezza, di integrità o di disponibilità);
- La natura, la delicatezza, nonché la mole dei Dati Personali violati in relazione ad un singolo individuo;
- La facilità di identificazione degli Interessati coinvolti;
- La gravità delle conseguenze per gli Interessati, nel caso in cui si verificasse la violazione;
- Caratteristiche particolari degli individui (ad esempio, maggiori rischi possono sussistere se i dati violati appartengono a minori, o soggetti vulnerabili), nonché del Titolare del trattamento (ad esempio, il rischio per gli individui può essere più grave se il Titolare del Trattamento è una struttura sanitaria);
- Il numero degli individui coinvolti (generalmente, maggiore è il numero dei soggetti coinvolti maggiori sono i rischi per gli stessi).

Il GDPR è chiaro nello stabilire che il Titolare deve procedere alla notifica all'autorità di vigilanza nel momento in cui sia consapevole dell'avvenuta violazione e tale violazione può comportare un rischio per gli Interessati. Ciò deve avvenire anche quando non sono ancora chiare tutte le informazioni

concernenti la violazione (ad esempio l'esatto numero degli Interessati coinvolti, tutte le categorie di dati personali violati). A tal proposito, il par. 4 dell'art. 33 stabilisce che qualora non sia possibile fornire tutte le informazioni della violazione all'atto di notifica all'autorità di vigilanza, gli ulteriori elementi di cui si venisse successivamente in possesso possono essere fornite in fasi successive senza ingiustificato ritardo.

9.1. Elementi della notificazione

La notificazione all'autorità di vigilanza deve contenere delle informazioni minime necessarie, quali:

- Descrizione della natura della violazione di Dati Personali;
- Se già disponibili, le categorie di Dati Personali coinvolte;
- Se disponibili, il numero anche approssimativo di Interessati coinvolti;
- Se previsto, i dati di contatto del Responsabile della Protezione dei Dati Personali o del Referente Privacy;
- Descrizione delle probabili conseguenze della violazione;
- Descrizione delle misure adottate e/o di quelle che si intendono implementare, al fine di rimediare alla violazione o, quantomeno, di limitarne gli effetti negativi.

10. Comunicazione della violazione agli Interessati

Ai sensi dell'art. 34 del GDPR se la violazione di Dati Personali è idonea ad arrecare un rischio elevato ai diritti e alle libertà delle persone coinvolte, il Titolare del Trattamento deve darne comunicazione all'Interessato senza ingiustificato ritardo.

A differenza di quanto previsto, per la notifica all'autorità di vigilanza, il GDPR non ha stabilito un termine perentorio per la comunicazione agli Interessati.

La comunicazione agli Interessati costituisce un obbligo solo se la violazione è suscettibile di presentare un rischio elevato per i diritti e per le libertà delle persone coinvolte. Inoltre, la comunicazione all'interessato non è necessaria se è soddisfatta una delle seguenti condizioni:

- Il Titolare del trattamento ha messo in atto delle misure tecniche e organizzative adeguate di protezione, le quali erano già state applicate per i Dati Personali oggetto di violazione (ad esempio, misure volte alla cifratura dei Dati Personali);
- Il Titolare del trattamento ha successivamente adottato misure volte a scongiurare la possibilità di verificazione di un rischio elevato per i diritti e le libertà degli Interessati;
- Se la comunicazione ai singoli Interessati richiedesse sforzi spropositati. In questo caso, la comunicazione ai singoli interessati può essere sostituita con una comunicazione pubblica o un mezzo assimilato.

Anche in tal caso, la valutazione circa la necessità di procedere o meno ad una comunicazione all'Interessato sarà rimessa al DPO.

La comunicazione agli Interessati dovrà descrivere con un linguaggio semplice e chiaro la natura della violazione dei Dati Personali e dovrà contenere almeno le seguenti informazioni:

- la natura della violazione dei Dati Personali, nonché le categorie e il numero approssimativo di registrazioni di Dati Personali oggetto della violazione;
- i dati di contatto del Responsabile della Protezione dei Dati Personali o, del Referente Privacy;
- le probabili conseguenze della violazione dei Dati Personali;
- le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione.

11. Documentazione dell'incidente nel registro delle violazioni

Ai sensi dell'art. 33, par. 5 GDPR, il Titolare del trattamento deve tenere traccia e documentare qualsiasi violazione di dati personali verificatasi, comprese le circostanze dell'incidente e le misure adottate per porvi rimedio. Il GDPR, dunque, impone l'adozione di una sorta di registro delle violazioni, nel quale annotare non solo gli incidenti che hanno provocato la necessità di una notifica all'autorità di vigilanza e/o agli Interessati, ma anche per quelle violazioni che non hanno prodotto un rischio per i diritti e le libertà degli interessati. La finalità della produzione di un tale registro è chiara, consentire al Titolare del trattamento di fornire una prova della legittimità delle azioni intraprese a seguito della violazione di dati personali.

La compilazione del registro delle violazioni verrà effettuata a cura del Referente Privacy, anche sulla base delle indicazioni del DPO.

Il presente regolamento è stato redatto in data _____

POLICY SULLA GESTIONE DEI DIRITTI DEGLI INTERESSATI

PREMESSE

La presente Policy è stata redatta nel rispetto del Regolamento europeo per la protezione dei dati personali n. 2016/679 (di seguito "GDPR"), che prevede, tra i suoi punti cardine, la tutela dei diritti dell'interessato nel trattamento dei dati personali.
Tali diritti consentono al soggetto interessato un controllo sulle tipologie dei dati utilizzati, sulle modalità di trattamento e gli conferisce la possibilità di limitare tale uso, di opporsi nonché di cancellare i dati personali in talune circostanze.
Corollario di tali diritti è il diritto al reclamo e alla tutela giudiziaria in caso di violazioni in tema di trattamento non consentito o illecito.
La presente procedura ("Procedura") disciplina la completa e corretta gestione delle richieste inoltrate a Extetica Group S.r.l. ("Società" o "Titolare") dai soggetti a cui i dati personali si riferiscono ("Interessati") relativamente ai diritti di cui al capo III del Regolamento (UE) 2016/679 ("GDPR"), definendo i ruoli e le responsabilità dei soggetti coinvolti nella Procedura, le condizioni e i limiti all'esercizio dei predetti diritti, nonché le modalità di riscontro all'Interessato.

Definizioni

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali.

Dato personale: qualsiasi informazione riguardante una persona fisica che sia identificata o comunque identificabile (ad esempio, dati anagrafici, numeri di telefono, indirizzi e-mail, indirizzo IP, numero di carta di credito).

Categorie particolari di dati personali: dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni filosofiche, o l'appartenenza sindacale, nonché dati sanitari, genetici, biometrici, relativi alla vita sessuale o all'orientamento sessuale di una persona.

Interessato: Persona fisica identificata o identificabile cui si riferiscono i dati personali.

Titolare del trattamento: 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.

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.

Responsabile della protezione dei dati (DPO): il *Data Protection Officer* è nominato dal titolare del trattamento e dal responsabile del trattamento secondo le prescrizioni di cui alla sezione 4 del Capo IV del GDPR

Referente di Area: figura di riferimento di ogni dipartimento e/o ufficio.

Referente Privacy: referente incaricato di assistere la Società, a livello locale, ai fini dell'adeguamento al GDPR ed ai fini dell'osservanza di tutte le normative vigenti in materia di privacy e di protezione dei dati personali

1. PRINCIPI GENERALI

Il Titolare del Trattamento ha adottato misure organizzative appropriate per fornire all'interessato tutte le informazioni e le comunicazioni di cui agli articoli da 13 a 22 e all'articolo 34 del GDPR al fine di fornire un riscontro in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, per garantire l'agevole esercizio dei predetti diritti.
La Società ha individuato al proprio interno una struttura organizzativa del flusso informativo per la gestione delle eventuali richieste degli Interessati in tema di privacy, indipendentemente dalla modalità con cui le stesse vengono avanzate (es. tramite richiesta cartacea, inviata tramite sistemi informatici o, se del caso, avanzata oralmente).

2. AMBITO DI APPLICAZIONE

La presente Procedura si applica alle richieste degli Interessati, avanzate ai sensi degli articoli 15 - 22 del GDPR, riguardanti i dati personali trattati, raccolti e/o conservati dalla Società in qualità di Titolare del trattamento.
Di conseguenza, la presente Procedura si applica alla gestione di tutte le diverse categorie di Interessati con cui la Società si interfaccia come Titolare, vale a dire dipendenti, collaboratori, stagisti, clienti, utenti web, visitatori, fornitori, etc.

3. GESTIONE E RISCONTRO DEI DIRITTI PREVISTI DAL GDPR

Le istanze ricevute andranno trasmesse dai singoli dipendenti, o il dipendente che riceva l'istanza, al proprio Referente di Area, che provvederà ad inoltrare la richiesta al Referente Privacy. Il Referente Privacy condividerà la richiesta ricevuta con il DPO, che la valuterà attentamente al fine di procedere al riscontro della stessa, con le modalità richieste dall'interessato, qualora possibili. Il DPO dovrà essere sempre coinvolto ed aggiornato, semmai, anche attraverso il contatto diretto con i Referenti di Area ove pervenga la richiesta, per valutare attentamente ogni circostanza utile per fornire riscontro all'interessato.
Il DPO, per poter svolgere i suoi compiti, potrà coinvolgere le singole persone che riterrà opportuno prima di procedere con il riscontro, occupandosi di chiedere ai soggetti coinvolti nella procedura di verificare sempre dell'identità dell'Interessato e di reperire tutte le informazioni richieste con il supporto dell'Ufficio Legale (Referente Privacy).
Una volta finalizzato, sarà cura del DPO, previo coordinamento con il Referente Privacy, procedere all'invio del riscontro all'Interessato con le modalità ritenute opportune o indicate dall'Interessato stesso, ove possibile.
Il riscontro dovrà avvenire entro un mese dal ricevimento della richiesta, prorogabile di un mese, ove necessario, tenuto conto della complessità e del numero delle richieste. In questo caso, entro un mese dalla richiesta, dovrà essere fornito riscontro all'interessato in merito alla necessità di proroga ed ai motivi del ritardo. In ogni caso, qualora l'esercizio dei diritti non rientri tra quelli previsti dal GDPR, sarà necessario sempre fornire riscontro all'interessato, illustrando i motivi per i quali non è possibile dar seguito all'istanza ricevuta dalla Società
Il Processo di gestione generale delle richieste degli interessati sarà suddiviso nei seguenti step:

1- Esercizio del diritto da parte dell'interessato
2- Ricezione richiesta da parte del dipendente
3- Trasmissione della richiesta dal dipendente al proprio Responsabile d'ufficio
4- Trasmissione del Responsabile al Referente Privacy
5- Coinvolgimento del DPO

6- Elaborazione della richiesta (verifica identità e reperimento informazioni)

Riscontro all'interessato da parte del DPO previo coordinamento con il Referente Privacy.

3.1. TEMPI

Il titolare del trattamento fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta ai sensi degli articoli da 15 a 22 senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tuttavia:

- 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. Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato.

- Se non ottempera alla richiesta dell'interessato, il titolare del trattamento informa l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale.

3.2. CASI DI RIGETTO

Il Titolare può rifiutare la richiesta avanzata dall'Interessato, dando comunque riscontro entro un mese dalla ricezione della richiesta:

- se dimostra di non essere in grado di identificare l'interessato, anche a seguito della richiesta integrativa inviata all'Interessato medesimo;

- se le richieste dell'interessato sono manifestamente infondate o eccessive (es. richieste ripetitive e pretestuose). In questo caso, la Società potrà decidere di:

a) addebitare all'Interessato un contributo ragionevole, tenuto conto dei costi amministrativi sostenuti per fornire le informazioni o intraprendere l'azione richiesta; oppure

b) rigettare la richiesta dell'Interessato, indicando i motivi dell'inottemperanza e della possibilità di proporre reclamo ad un'autorità di controllo o di proporre ricorso giurisdizionale.

3.3. COSTI

L'esercizio dei diritti previsti dal GDPR è gratuito. Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento può:

a) addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta; oppure

b) rifiutare di soddisfare la richiesta.

Il GDPR prevede che incombe al titolare del trattamento l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

4. I DIRITTI DEGLI INTERESSATI

La Società ha adottato idonee misure organizzative al fine di gestire e riscontrare adeguatamente l'esercizio dei seguenti diritti riconosciuti agli Interessati dal GDPR:

A. Diritto di accesso ai dati;

B. Diritto di rettifica;

C. Diritto alla cancellazione (diritto “all’oblio”);
D. Diritto di limitazione del trattamento;
E. Diritto alla portabilità dei dati;
F. Diritto di opposizione al trattamento;
G. Diritto di opposizione al trattamento di profilazione (o a qualsiasi altro processo decisionale automatizzato).

A. DIRITTO DI ACCESSO AI DATI (ART. 15 GDPR)

L'Interessato ha il diritto di chiedere al 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 e alle seguenti informazioni relative al trattamento in corso. Se la richiesta è generica occorrerà fornire le seguenti informazioni:

a) le finalità del trattamento;
b) le categorie di dati personali coinvolti nel trattamento;
c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, indicando inoltre se la comunicazione dei dati comporta un trasferimento in Paesi Extra-UE degli stessi;
d) quando possibile, il periodo di conservazione dei dati personali previsto oppure i criteri utilizzati per determinare tale periodo;
e) esistenza del diritto dell’interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
f) il diritto di proporre reclamo a un’autorità di controllo;
g) qualora i dati non siano raccolti direttamente presso l’Interessato, le informazioni circa l’origine dei dati personali dell’Interessato;
h) l’esistenza di un processo decisionale automatizzato (vale a dire, una decisione basata unicamente su un’elaborazione automatizzata di dati personali), compresa la profilazione, nonché informazioni circa la logica utilizzata, l'importanza e le conseguenze di un simile trattamento per l’Interessato.

Qualora i dati personali siano trasferiti a un paese terzo o a un’organizzazione internazionale, l’Interessato ha anche il diritto di essere informato circa le garanzie adeguate adottate dal Titolare al fine di legittimare tale trasferimento, a titolo esemplificativo: la richiesta del consenso, l’adozione di appositi Data Transfer Agreement (c.d. Clausole Contrattuali Standard approvate dalla Commissione Europea), l’adesione da parte del destinatario al regime del Privacy Shield US - EU, oppure ove applicabile l’eventuale implementazione di apposite Binding Corporate Rules per i trasferimenti infra-gruppo.

Il Titolare del trattamento deve fornire una copia dei dati personali oggetto di trattamento; qualora l'Interessato presenti la richiesta mediante mezzi elettronici (es. via email), e salvo indicazione diversa dell'Interessato stesso, le informazioni sono fornite in un formato elettronico di uso comune (es. pdf).

Attenzione - Limitazione all’esercizio del diritto di accesso:
Il diritto di accesso, e quindi di ottenere copia dei dati personali oggetto di trattamento, non deve ledere i diritti e le libertà altrui.

B. DIRITTO DI RETTIFICA DEI DATI (ART. 16 GDPR)

L'Interessato ha il diritto di richiedere al Titolare del trattamento:

- la rettifica e/o aggiornamento dei dati personali che lo riguardano qualora siano inesatti;
- l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

L'esercizio del diritto di rettifica non opera rispetto a dati valutativi e soggettivi (es. appunti e annotazioni predisposti in sede di colloquio del candidato).
Al fine di garantire il corretto adempimento dell'esercizio del diritto di rettifica degli interessati, il Titolare è tenuto a comunicare ai destinatari, una volta effettuate le attività di rettifica ed integrazione, le modifiche effettuate, salvo che ciò si rilevi impossibile o implichi uno sforzo sproporzionato.

C. DIRITTO ALLA CANCELLAZIONE DEI DATI ("DIRITTO ALL'OBLIO") (ART. 17 GDPR)

L'Interessato ha il diritto di chiedere al Titolare la cancellazione dei dati personali che lo riguardano e il Titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, qualora sussiste uno dei seguenti motivi:

a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

b) l'Interessato revoca il consenso su cui si basa il trattamento, conforme alle condizioni di liceità di cui all'art. 6, par. 1 lett. a) e art. 9, par. 2 lett. a) rilasciato per una o più specifiche finalità (es. attività di marketing, raccolta di categorie particolari di dati) e non sussiste altra base giuridica su cui si possa fondare lecitamente un trattamento;

c) l'Interessato si oppone al trattamento dei suoi dati personali basato sul legittimo interesse del Titolare o su motivi di interesse pubblico, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure l'interessato si oppone al marketing diretto;

d) i dati personali sono stati trattati illecitamente;

e) i dati personali devono essere cancellati per adempiere un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare;

f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione (es. internet) relativi a minori di età inferiore a 14 anni.

Il titolare del trattamento, tenendo conto della tecnologia disponibile e dei costi di attuazione, se ha reso pubblici dati personali e successivamente sia obbligato a cancellarli, adotta misure ragionevoli, anche tecniche, per informare i titolari del trattamento, destinatari dei dati, di cancellare qualsiasi link, copia o riproduzione degli stessi perché oggetto di una richiesta di cancellazione.

ECCEZIONI ALLA CANCELLAZIONE

Il GDPR prevede alcune eccezioni al diritto di cancellazione dei dati.
In particolare, l'Interessato non può esercitare il diritto di cancellazione qualora ricorra una delle seguenti ipotesi:

- il trattamento dei dati personali è effettuato per l'esercizio del diritto alla libertà di espressione e informazione (c.d. bilanciamento di interessi);
- il trattamento è effettuato per l'adempimento di un obbligo di legge, regolamento, normativa nazionale o UE, o per l'esecuzione di un compito svolto nel pubblico interesse;
- il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica;
- il trattamento è necessario ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, nella misura in cui il diritto di alla cancellazione rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento.

- il trattamento è effettuato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

D. DIRITTO ALLA LIMITAZIONE DEL TRATTAMENTO (ART. 18 GDPR)

L'Interessato ha il diritto di chiedere al Titolare una restrizione (limitazione) al trattamento dei dati solo quando ricorra una delle seguenti ipotesi:

a) l'Interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare per verificare l'esattezza di tali dati personali;

b) il trattamento è illecito e l'Interessato si oppone alla cancellazione chiedendo che ne sia limitato l'utilizzo;

c) i dati personali sono necessari all'Interessato per l'accertamento e l'esercizio di difesa in sede giudiziaria, benché il Titolare non ne abbia più bisogno;

d) l'Interessato si è opposto al trattamento, in attesa della verifica in merito all'eventuale prevalenza dei legittimi motivi del Titolare rispetto a quelli dell'Interessato.

ECCEZIONI ALLA LIMITAZIONE DEL TRATTAMENTO

Il GDPR prevede alcune eccezioni al diritto di limitazione del trattamento dei dati.

In particolare, l'Interessato non può esercitare il diritto di limitazione qualora ricorra una delle seguenti ipotesi:

- l'Interessato presta il consenso all'ulteriore trattamento dei dati personali oggetto della richiesta di limitazione;
- il trattamento dei dati è necessario per l'adempimento di un obbligo di legge, regolamento, normativa nazionale o UE, o per l'esecuzione di un compito svolto nel pubblico interesse;
- per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria o per tutelare i diritti di un'altra persona fisica o giuridica.

L'interessato è informato se il trattamento è effettuato sulla base di una delle suddette eccezioni.

L'interessato che ottiene la limitazione, dovrà essere informato circa la durata del periodo di eventuale limitazione del trattamento ottenuta, prima che sia revocata.

E. DIRITTO ALLA PORTABILITÀ DEI DATI (ART. 20 GDPR)

L'Interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico (es. in formato pdf.) i dati personali che lo riguardano forniti al Titolare del trattamento qualora:

a) il trattamento si basi sul consenso espresso per una o più specifiche finalità;

b) il trattamento sia necessario all'esecuzione di un contratto di cui l'Interessato è parte o delle relative misure precontrattuali (es. dipendente in relazione al contratto di lavoro); e

c) il trattamento sia effettuato con mezzi automatizzati.

Nel richiedere la portabilità dei dati, l'Interessato ha anche il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.

ECCEZIONI ALLA PORTABILITÀ

Il GDPR prevede alcune eccezioni al diritto di portabilità dei dati. Tale diritto, infatti, non potrà essere esercitato quando il trattamento dei dati personali oggetto della richiesta di portabilità:

- è svolto attraverso mezzi cartacei;
- è necessario per l'adempimento di un obbligo di legge, regolamento, normativa nazionale o UE, o per l'esecuzione di un compito svolto nel pubblico interesse;

- è necessario per la salvaguardia degli interessi vitali dell'Interessato o di un'altra persona fisica;
- a fini di ricerca scientifica o storica o a fini statistici, secondo la legge nazionale;
- è necessario per il perseguimento del legittimo interesse del Titolare del trattamento o di terzi (ivi incluso in caso di contenziosi), a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'Interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore;
- I dati personali sono generati dal Titolare (utilizzando come input i dati osservati o forniti direttamente);
- Quando lede diritti e le libertà altrui.

F. DIRITTO DI OPPOSIZIONE AL TRATTAMENTO (ART. 21 GDPR)

L'Interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare:

(i) al trattamento dei dati personali che lo riguardano per scopi di interesse pubblico o per legittimo interesse, compresa la profilazione.

Il Titolare è tenuto a confrontare gli interessi dell'Interessato rispetto a propri al fine di dimostrare la sussistenza dei motivi che consentono il trattamento. L'analisi sarà effettuata con il coinvolgimento del DPO. Di quest'analisi verrà redatto apposito documento di valutazione.

Qualora il confronto stabilisca la prevalenza delle ragioni dell'Interessato, la Società dovrà astenersi dal trattare ulteriormente i dati personali.

(ii) Ai trattamenti di marketing diretto, compresa la profilazione, se connessa all'attività di marketing diretto.

G. DIRITTO DI OPPOSIZIONE A PROCESSO DECISIONALE AUTOMATIZZATO, COMPRESA LA PROFILAZIONE (ART. 22 GDPR)

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 (es. rifiuto di un rifiuto automatico di una domanda di credito online o pratiche di recruiting elettronico senza interventi umani). Tale diritto non si applica quando il trattamento/la decisione:

a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'Interessato e il Titolare del trattamento;

b) sia autorizzata dal diritto nazionale o UE cui è soggetto il Titolare del trattamento;

c) si basi sul consenso esplicito dell'Interessato.

Nei casi sub a) e c), il Titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, tra cui almeno il diritto di ottenere l'intervento umano da parte del Titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.

Il presente regolamento è stato redatto in data _____