ELIOR GROUP

Politica sulla protezione dei dati personali

Perimetro	Tutti i perimetri
Versione	V1
Redattore	Comitato operativo DCP
Convalidatore	Comitato direttivo DCP
Data di pubblicazione	01/03/2019
Ultimo aggiornamento	

Introduzione

La presente politica di protezione dei dati personali definisce le modalità con cui il gruppo Elior procede al momento dell'attuazione del trattamento dei dati personali per garantire la tutela dei diritti e delle libertà fondamentali delle persone fisiche, in particolare il loro diritto alla protezione dei dati personale.

Definisce le norme che tutti i collaboratori, collaboratrici, partner e subappaltatori del Gruppo Elior devono rispettare quando trattano dati personali.

Si ricorda che il mancato rispetto degli obblighi in materia di protezione dei dati personali espone il gruppo Elior a una sanzione del 4% del suo fatturato mondiale; a titolo indicativo, ciò rappresenta circa 268 milioni di euro sulla base dei risultati dell'esercizio chiuso al 30 settembre 2018.

Ognuno degli interessati deve in particolare garantire:

- il rispetto del principio di tutela della vita privata sin dalla progettazione di nuovi progetti (*privacy by design*) e in particolare che ogni trattamento di dati (i) corrisponda a una finalità delimitata, (ii) preveda di informare le persone del trattamento dei dati attuato, (iii) determini misure di protezione e (iv) fissi una durata di conservazione dei dati personali;
- il rispetto dei termini previsti per la risposta alle richieste di esercizio dei diritti, vale a dire un mese, e la notifica di eventuali fughe di dati alle autorità competenti entro 72 ore;
- più in generale, il rispetto dei processi e delle raccomandazioni posti in essere dalla presente politica e la richiesta, se del caso, degli ambasciatori di protezione dei dati personali o del team GDPR del Gruppo Elior tramite l'indirizzo gdpr-contact@eliorgroup.com.

Glossario

« **gruppo Elior »** indica la società Elior Group e tutte le società che, ai sensi dell'articolo L233-3 del Codice di Commercio,

(i) sono sotto il controllo diretto o indiretto della società Elior Group o,

(ii) sono, direttamente o indirettamente, sotto il controllo comune con la società Elior Group;

« **dati di carattere personale »**,« **dati personali** » oppure " **DCP** indica qualsiasi informazione relativa a una persona fisica identificata o identificabile (di seguito, « **interessato** »). Si intende essere una "persona fisica identificabile" una persona fisica che può essere identificata, direttamente o indirettamente, in particolare con riferimento a un identificativo come un nome, un numero di identificazione, dati di localizzazione, un identificativo online, o a uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

« **elaborazione di dati »** indica qualsiasi operazione o insieme di operazioni effettuate o meno con processi automatizzati e applicate a dati o insiemi di dati personali, quali la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'utilizzo, la comunicazione mediante trasmissione, la diffusione o altre forme di messa a disposizione, il collegamento o l'interconnessione, la limitazione, la cancellazione o la distruzione;

« **titolare del trattamento »** indica la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che, da solo o congiuntamente ad altri, determina le finalità e i mezzi del trattamento; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione europea o dal diritto di uno Stato membro, il titolare del trattamento può essere designato o i criteri specifici applicabili alla sua designazione possono essere previsti dal diritto dell'Unione europea o dal diritto di uno Stato membro;

« **subappaltatore** » indica la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che tratta dati personali per conto del titolare del trattamento;

« **titolare SI del trattamento** indica il collaboratore all'interno del gruppo Elior, garante delle conoscenze tecniche relative alle risorse informatiche coinvolte nel trattamento, per ogni trattamento di DCP individuato all'interno del gruppo Elior;

« **responsabile attività di trattamento** » indica il collaboratore all'interno del gruppo Elior, che definisce le esigenze professionali e gli obiettivi (committenza) del trattamento, e ciò per ogni trattamento di dati individuato all'interno del gruppo Elior;

« **destinatario »** indica la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che riceve comunicazione di dati personali, indipendentemente dal fatto che tale destinatario sia o meno esterno al gruppo Elior (terzo). Tuttavia, le autorità pubbliche che possono ricevere comunicazioni di dati personali nel quadro di una specifica missione d'inchiesta non sono considerate destinatari; il trattamento di dati personali da parte di tali autorità è conforme alle norme applicabili in materia di protezione dei dati in funzione delle finalità del trattamento;

« **consenso [dell'interessato] »** indica qualsiasi manifestazione di volontà, libera, specifica, informata e univoca, con la quale il soggetto i cui dati personali sono trattati accetta, con dichiarazione o con atto positivo chiaro, che tali dati siano oggetto di trattamento;

« **violazione di dati personali** » si intende una violazione della sicurezza che comporti, in modo accidentale o illecito, distruzione, perdita, alterazione o infine divulgazione non autorizzata di dati personali trasmessi, conservati o trattati in altro modo, oppure accesso non autorizzato a tali dati;

« **regole aziendali vincolanti** » o « **Binding Corporate Rules** » o « **BCR »** indica una politica di protezione dei dati intra-Gruppo nell'ambito di qualsiasi trasferimento di dati personali realizzato, in tutto o in parte, lo Spazio economico europeo. Sono giuridicamente vincolanti e rispettate dalle entità firmatarie di un gruppo di società, a prescindere dal loro paese di insediamento, nonché da tutti i dipendenti di una stessa entità giuridica o di uno stesso gruppo di società. Esistono due tipi di BCR : (i) le BCR

"titolare del trattamento", che consentono di inquadrare i trasferimenti effettuati all'interno di un gruppo che agisce in qualità di titolare del trattamento, e (ii) le BCR « subappaltatore », che consentono di creare una sfera di sicurezza per i trasferimenti effettuati quando il gruppo agisce in qualità di subappaltatore;

« **valutazione di impatto sulla protezione dei dati** » o « **Data Protection Impact Assessment** » o « **DPIA** » significa che il titolare del trattamento, prima di qualsiasi trattamento che possa comportare un rischio elevato per i diritti e le libertà delle persone fisiche, in particolare avvalendosi di nuove tecnologie, realizza un'analisi d'impatto delle operazioni di trattamento previste sulla protezione dei dati personali. Una sola analisi può riguardare una serie di operazioni di trattamento simili che presentano rischi elevati simili.

Indice

1. Contesto

In quanto fornitore di servizi di ristorazione, la sicurezza alimentare costituisce un aspetto fondamentale dell'attività del gruppo Elior. Proporre un'alimentazione sana, preparata e distribuita conformemente alla normativa vigente ai suoi clienti e ospiti è una preoccupazione costante per il gruppo Elior e costituisce uno dei fondamenti della fiducia da essi accordatagli. Su questa stessa base, realizzare trattamenti di dati personali conformi alla legislazione vigente costituisce una sfida fondamentale per il gruppo Elior.

In effetti, la rapida evoluzione delle tecnologie e la globalizzazione hanno portato a un aumento sostanziale dei flussi di scambio di dati personali tra gli operatori, il che si traduce in nuove sfide per la protezione dei DCP. La portata della raccolta e della condivisione dei dati personali è aumentata in modo significativo, favorendo un utilizzo e una valorizzazione di questi dati senza precedenti. Il gruppo Elior, la cui ambizione è di differenziarsi per l'innovazione tecnologica nel settore del digitale e per una crescente capacità di raccogliere e sfruttare dati, si inserisce pienamente in questa tendenza. I dati sono onnipresenti e ormai posizionati al centro della catena di creazione di valore. Ben gestiti e tutelati, consentono di aumentare l'efficienza e la competitività, di personalizzare e consolidare il rapporto con i clienti e gli ospiti, di conquistare nuovi mercati, di migliorare i prodotti e i servizi e di facilitare la collaborazione e la mobilità.

Ciò non può avvenire senza stabilire la fiducia che consentirà al posizionamento digitale del gruppo Elior di svilupparsi, garantendo ai team, ai clienti, agli ospiti e, più in generale, a tutti gli interlocutori del gruppo Elior, il controllo dei dati personali che li riguardano.

Di fronte all'emergere di quadri legislativi nazionali e sovranazionali, il gruppo Elior si impegna costantemente ad adattarsi alle sfide del digitale e a creare un processo di miglioramento continuo e di adeguamento della gestione dei dati personali.

2. Perimetro

Il gruppo Elior tratta costantemente dati personali nell'ambito delle proprie attività, ad esempio:

- durante la cattura di immagini mediante videosorveglianza;
- durante il trattamento di richieste formulate dai clienti;
- durante la raccolta dei regimi alimentari degli ospiti al fine di servire loro pasti adeguati;
- oppure, al momento della raccolta di informazioni sui team nell'ambito della gestione delle loro carriere.

La presente politica si applica a tutti i collaboratori, collaboratrici, partner e subappaltatori del gruppo Elior, ogni volta che vengono raccolti, utilizzati, resi accessibili o condivisi dai dipendenti dei dati personali relativi a clienti, ospiti, team, fornitori o altre persone fisiche.

Data l'ubicazione della sede legale del gruppo Elior in Francia, questa politica mira in particolare a rispondere agli obblighi posti in essere dal regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche riguardo il trattamento dei dati personali e la libera circolazione di tali dati, di seguito "Regolamento generale sulla protezione dei dati", "Regolamento" o "RGPD".

Questo approccio s'iscrive nella volontà di armonizzare dall'alto le pratiche all'interno del gruppo Elior, di semplificare il monitoraggio e il mantenimento nel tempo della conformità e di garantire un livello elevato di protezione dei dati personali. Per raggiungere tale obiettivo, la presente politica deve tener conto, per quanto possibile, delle specificità nazionali:

- all'interno dello Spazio economico europeo, parallelamente Regolamento generale sulla protezione dei dati, mediante il rispetto delle disposizioni legislative nazionali specifiche che precisano le condizioni in cui il trattamento dei dati personali è lecito;
- al di fuori dello Spazio economico europeo, mediante la presa in considerazione in tutti gli Stati all'interno dei quali il gruppo Elior è presente di una legislazione nazionale dedicata alla protezione dei dati di carattere personale, ovvero di un'autorità specificamente competente per la sua applicazione.

É bene precisare che il diritto alla protezione dei dati personali non è un diritto assoluto, deve essere considerato in relazione alla sua funzione nella società e deve essere soppesato rispetto ad altri diritti fondamentali, conformemente al principio di proporzionalità, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e di informazione o, infine, la libertà imprenditoriale. Questa politica non è intesa a definire l'equilibrio tra questi diritti, che dovrà essere valutato caso per caso dai servizi giuridici del gruppo Elior rispetto all'evoluzione della giurisprudenza e delle raccomandazioni delle autorità.

3. Governance

A. Quadro generale

Il processo di gestione dei dati è guidato da un **team Gruppo** composto da:

- Un **Group Chief Compliance Officer**: collegato direttamente al direttore generale, è responsabile dell'attuazione delle regole di conformità. È il garante della presa in considerazione, a un livello ottimale, della protezione dei dati personali all'interno del gruppo Elior;

- Un **Group Data Protection Officer** (DPO): è garante dell'attuazione del programma di protezione dei dati personali e del rispetto della legislazione associata per tutto il gruppo Elior. Dispone di una buona conoscenza delle attività e dell'organizzazione del gruppo Elior, in particolare delle operazioni di trattamento, dei sistemi informativi e delle esigenze del gruppo Elior in materia di protezione e sicurezza dei dati. Esercita le sue funzioni e svolge le sue missioni in piena indipendenza e può contare su un supporto **Group IT Security Compliance Manager**.

- Un **Group Senior Legal Counsel**: accompagna e consiglia il DPO nella comprensione e nell'interpretazione dei testi giuridici e nel rapporto con le autorità di protezione dei dati personali. Inoltre, è garante della presa in considerazione di problematiche di protezione dei dati personali nell'ambito dei rapporti contrattuali.

Il team Gruppo si basa su attori decentralizzati nel gruppo Elior: gli **ambasciatori DCP**. Questi ambasciatori DCP sono il portavoce del DPO all'interno del loro perimetro e contribuiscono in particolare:

- alla definizione delle politiche e delle procedure associate;
- alla garanzia della conformità alla politica del Gruppo, in particolare rispetto all'esercizio dei diritti e alla tenuta del registro dei trattamenti;
- a essere i punti di contatto privilegiati nei confronti del team RGPD Gruppo e del loro perimetro per qualsiasi questione relativa ai DCP.

La presente politica è rivista su base annuale, su iniziativa del team RGPD Gruppo al fine di tenere conto di qualsiasi evoluzione della legislazione o delle pratiche interne all'interno del gruppo Elior. Ogni controllata del gruppo Elior è libera di organizzarsi internamente e di declinare la presente politica per facilitarne la diffusione e l'applicazione.

B. Strumento per la conformità

Il gruppo Elior si è recentemente dotato di un software di gestione della conformità, che consente di soddisfare gli obblighi relativi alla protezione dei dati personali e di gestire le procedure associate o anche di accompagnare i propri team nel rispetto delle regole di conformità nell'ambito delle loro attività.

Tutti i collaboratori del gruppo Elior chiamati ad avere responsabilità in materia di trattamento dei dati personali (ossia i responsabili SI e attività nonché gli ambasciatori DCP) dispongono di un accesso a tale ambiente. Questo strumento consente in particolare di:

- tenere aggiornati i registri di trattamento (titolare del trattamento/subappaltatori);
- affiancare i responsabili di progetto nell'applicazione delle esigenze relative alla protezione dei dati;
- generare moduli di contatto per l'esercizio dei diritti delle persone e gestirne il trattamento;
- mantenere un registro dei subappaltatori;
- gestire le notifiche di incidenti;
- più in generale permettere il rispetto della legislazione all'interno del gruppo Elior conformemente al principio di responsabilizzazione.

È tuttavia responsabilità:

- dei capi progetto (responsabile SI e responsabile attività) compilare ogni nuovo trattamento dati all'interno di tale ambiente e degli ambasciatori DCP accompagnare e convalidare le informazioni fornite;
- degli ambasciatori DCP garantire il corretto trattamento delle domande di esercizio dei diritti con il supporto dei responsabili SI e attività.

C. Comitato direttivo DCP (CP DCP)

Condotto dal DPO e sotto la presidenza del Group Chief Compliance Officer, il comitato direttivo dei dati personali è l'organo decisionale.

Ha in particolare le seguenti attribuzioni relative alla protezione dei dati personali all'interno del gruppo Elior:

- convalidare la politica e le sue evoluzioni;
- stilare il bilancio annuale delle azioni;
- prendere atto del livello di conformità;
- confermare e valutare la priorità delle azioni.

A integrazione del team Gruppo, il CP DCP è composto dai seguenti membri:

- il direttore dei sistemi informativi del Gruppo;
- il direttore legale del Gruppo;
- il direttore dell'audit interno del Gruppo;
- il direttore assicurazioni e prevenzione dei rischi Gruppo;
- i direttori dei sistemi informativi delle operazioni;
- i direttori legali operazioni.

Una raccolta delle decisioni del CP sarà formalizzata dal DPO al termine dei comitati. I verbali saranno accessibili a tutte le parti interessate.

Il CP DCP si riunisce su base annuale. Può riunirsi straordinariamente in occasione di un evento ritenuto significativo, su proposta del DPO (incidente di rilievo, arbitrato importante, controllo delle autorità...).

D. Gruppo di lavoro sulla protezione dei dati personali (GL)

Condotto dal IT Security Compliance Manager e dal Gruppo Senior Legal Counsel sotto la presidenza del DPO, il comitato operativo DCP è l'istanza di pianificazione e monitoraggio delle raccomandazioni formulate dal CP.

A complemento del team Gruppo, sono presenti anche gli ambasciatori DCP delle zone (ristorazione collettiva, ristorazione di concessione e servizi) e, se del caso, degli ambasciatori DCP a livello internazionale.

Il CO DCP si riunisce se del caso.

E. Conduzione trasversale

L' IT Security Compliance Manager è responsabile della conduzione dei lavori relativi alla protezione dei dati personali in Francia e a livello internazionale. Inoltre, provvede a identificare e diffondere le buone pratiche associate all'interno del gruppo Elior.

4. I nostri obblighi

La presente sezione descrive i vari obblighi legati alla protezione dei dati personali che spettano al gruppo Elior.

A. Responsabilità e inventari dei trattamenti

Il Regolamento generale sulla protezione dei dati introduce il principio di responsabilizzazione, o *accountability*, per il trattamento dei dati. Dalla sua entrata in vigore, il gruppo Elior deve essere in grado di dimostrare la propria conformità al regolamento; ciò richiede in particolare la realizzazione dell'inventario dei trattamenti di dati effettuati.

Quindi, all'interno del gruppo Elior si devono conservare due tipi di registri; il primo riguarda i trattamenti per i quali ogni entità del gruppo Elior è responsabile del trattamento; il secondo riguarda i trattamenti per i quali ogni entità del gruppo Elior agisce in qualità di subappaltatore.

Per ciascuno dei trattamenti per i quali il gruppo Elior agisce in qualità di titolare del trattamento, il registro deve contenere le seguenti informazioni:

- l'identità del titolare del trattamento e dei subappaltatori;
- l'identità e i dati dei responsabili SI e attività;
- la finalità (l'obiettivo perseguito dalla raccolta e dal trattamento dei dati);
- la base giuridica del trattamento;
- l'elenco dei dati raccolti, il loro periodo di conservazione e gli interessati;
- le categorie di persone che hanno accesso ai dati (amministratore, risorse umane, subappaltatori...);
- la presenza di trasferimento verso un paese terzo;
- la modalità in cui si effettua l'informazione delle persone;
- le misure di sicurezza attuate;

- eventualmente, i risultati della DPIA.

Per ciascuno dei trattamenti per i quali il gruppo Elior agisce in qualità di subappaltatore, il registro deve contenere le seguenti informazioni:

- il nome e i dati di ogni cliente per conto del quale sono trattati i dati;
- il nome e i dati di ogni subappaltatore successivo, se del caso;
- le categorie dei trattamenti effettuati per conto di ciascun cliente;
- i trasferimenti di dati fuori dall'UE effettuati per conto del cliente;
- per quanto possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative messe in atto.

È competenza dei responsabili SI e attività compilare tale registro avvalendosi dei loro ambasciatori DCP.

B. Trasparenza e lealtà

Trasparenza

Il gruppo Elior e i suoi team hanno il dovere di essere chiari e trasparenti sui trattamenti di dati personali. I dati raccolti non devono essere utilizzati in un modo e con un obiettivo che non sia ragionevolmente atteso e previsto rispetto alla finalità perseguita.

Pertanto, prima di raccogliere dati personali, è opportuno comunicare con un linguaggio semplice e chiaro riguardo:

- chi siamo;
- quali sono i dati personali raccolti e quale ne è la fonte;
- le operazioni che saranno effettuate con tali dati personali e la base giuridica;
- se i dati personali sono o saranno condivisi con altri destinatari;
- il periodo di conservazione dei dati personali;
- se i dati personali saranno trasferiti al di fuori dello Spazio economico europeo;
- i diritti garantiti ai soggetti relativi al trattamento di dati personali.

Liceità del trattamento

Affinché il trattamento di dati personali sia lecito, è necessario avere motivi legittimi o motivare obblighi di natura legare oppure aver ottenuto il consenso dell'interessato. Pertanto, prima di qualsiasi trattamento di dati personali, a integrazione delle informazioni delle persone, occorre assicurarsi che quest'ultimo si basi su uno dei seguenti fondamenti:

- **Obbligo legale**: il trattamento è necessario al rispetto di un obbligo legale cui è soggetto il titolare del trattamento (diritto nazionale o diritto dell'Unione Europea); ad esempio, la comunicazione alla previdenza sociale e all'amministrazione fiscale dei dati relativi alla retribuzione dei dipendenti.

- **Necessità contrattuale**: il trattamento è necessario per l'esecuzione di un contratto di cui l'interessato è parte o per l'esecuzione di misure precontrattuali assunte su sua richiesta.
  Questa situazione deve coprire esclusivamente i servizi essenziali per la realizzazione del contratto e, in particolare, escludere qualsiasi attività di promozione commerciale; ad esempio, la raccolta dei dati di un ospite per l'emissione e l'invio di fatture oppure il trattamento di dati dei dipendenti per l'esecuzione del pagamento.

- **Interessi legittimi**: il trattamento è necessario ai fini degli interessi legittimi perseguiti dal titolare o da un terzo, a meno che non prevalgano gli interessi o le libertà e i diritti fondamentali dell'interessato che richiedono una protezione dei dati personali. In tal caso, il legittimo interesse del curatore deve essere sistematicamente soppesato rispetto ai diritti e alle libertà fondamentali degli interessati; ad esempio, la comunicazione di elementi legati alla corruzione ad un'autorità al di fuori dell'Unione europea o l'analisi del traffico per prevenire l'accesso a sistemi maligni per garantire la sicurezza della rete informatica.

- **Interessi vitali**: il trattamento è necessario per salvaguardare gli interessi vitali dell'interessato o di un'altra persona fisica; ad esempio, la raccolta di un numero di telefono personale per l'invio di SMS di allerta in caso di eventi gravi sul posto di lavoro o la raccolta di dati relativi a una dieta specifica per prevenire qualsiasi rischio per la salute di una persona.

- **Interesse pubblico**: questa base giuridica riguarda la situazione in cui il responsabile del trattamento è investito di un'autorità pubblica o di una missione di interesse pubblico, per la quale il trattamento è necessario. Nel caso in cui si verificasse tale situazione, questa base giuridica deve essere utilizzata caso per caso, previa convalida di un ambasciatore DCP.

- **Raccolta del consenso**: l'interessato ha acconsentito al trattamento dei propri dati personali per una o più finalità specifiche:
    - Il suo consenso deve essere libero (scelta reale, senza conseguenze negative), specifico (consenso specifico per ciascuna finalità), illuminato (presenza, al momento dell'espressione del consenso, di informazioni adeguate e sufficienti) ed univoca (logica di "opt-in", nessuna ambiguità e assenza di consenso per difetto o legato a inazione);
    - la raccolta del consenso deve poter essere dimostrabile (es.: casella da spuntare, modulo da compilare, procedure o meccanismi sistematici) e dare alla persona la possibilità di revocarlo.

Minimizzazione dei dati

Inoltre, le informazioni raccolte e registrate devono essere pertinenti e strettamente necessarie all'obiettivo perseguito. Pertanto, si devono adottare misure volte a ridurre al minimo il volume di dati personali raccolti e accertarsi che siano adeguate rispetto alla realizzazione delle finalità del trattamento.

C. Mantenere dati esatti e conservarli per un periodo limitato

Disporre di informazioni errate o inesatte su una persona può essere all'origine di eventuali danni. Ad esempio, una persona potrebbe essere esclusa dai vantaggi o dai benefici derivanti dal suo status. Occorre quindi essere particolarmente vigili quando si prende una decisione basandosi su dati personali.

Esattezza dei dati

I collaboratori del gruppo Elior devono accertarsi che le informazioni detenute siano esatte, il che è garantito in particolare dall'attuazione dei seguenti meccanismi:

- verificare l'esattezza delle informazioni al momento della raccolta, ove possibile;
- per quanto possibile, dare la possibilità agli interessati di aggiornare i dati che li riguardano;
- riesaminare periodicamente i dati personali conservati per accertarsi che restino aggiornati;
- correggere o eliminare i dati inesatti.

Rischi inerenti alle zone riservate ai liberi commenti (ZLC)

I campi di testo e le zone di commento devono essere oggetto di precauzioni particolari. Questi campi di testo liberi sono utili per garantire il monitoraggio di una pratica o per personalizzare un rapporto. Se non è vietato ricorrervi, il loro utilizzo deve essere regolato da azioni di sensibilizzazione e regole di gestione, per evitare che i commenti digitati possano violare i diritti degli interessati.

Alcuni commenti potrebbero rivelarsi denigratori, discriminanti, persino ingiuriosi, oppure potrebbero far apparire dati cosiddetti sensibili, come i dati sulla salute. I commenti devono quindi essere adeguati, obiettivi e rispettosi.

La miglior precauzione consiste nel ricordare che gli interessati (clienti, ospiti, dipendenti...) possono, in qualsiasi momento e su semplice richiesta, accedere al contenuto di queste zone commenti esercitando il loro diritto di accesso.

Periodo di conservazione

I dati personali non possono essere conservati a tempo indefinito, pertanto si deve stabilire un periodo di conservazione in funzione dell'obiettivo che ha condotto alla raccolta di tali dati. Una volta raggiunto questo obiettivo, questi dati devono essere archiviati, eliminati o resi anonimi (in particolare per produrre statistiche), a seconda del caso.

È importante notare che, nell'interesse legittimo del gruppo Elior e nella difesa dei suoi interessi, tali dati potranno tuttavia essere conservati per periodi più lunghi, giustificati da un contesto specifico, nell'ambito di contenziosi, ad esempio, e in ogni caso previa comunicazione al DPO.

D. Garantire la sicurezza dei dati

La sicurezza dei dati è una questione fondamentale per il gruppo Elior. Il fatto di non garantire la sicurezza dei dati per il loro intero ciclo di vita, dalla raccolta alla distruzione, può comportare gravi danni per i soggetti. Occorre prestare la massima attenzione alla sicurezza dei fornitori esterni quando questi ultimi sono parti interessate in un trattamento di dati personali.

Esistono vari modi per proteggere i dati personali, siano essi conservati in formato elettronico o cartaceo. Per assistere i propri collaboratori, il gruppo Elior mantiene a loro disposizione un corpus documentale conforme allo stato dell'arte, la cui applicazione è obbligatoria:

- una politica di sicurezza dei sistemi informativi e delle direttive associate che specifichino i requisiti applicabili ai sistemi informativi del gruppo Elior;
- requisiti di sicurezza che sono un prerequisito per qualsiasi contratto con un fornitore di servizi informatici.

le raccomandazioni presentate di seguito sono adeguate caso per caso e in funzione dei rischi derivanti dal trattamento di dati sulla privacy e sulla libertà degli interessati:

- le applicazioni devono essere protette mediante sistemi di autenticazione (ID e password) in conformità alla politica di sicurezza dell'informazione;
- l'accesso ai dati di carattere personale è consentito unicamente alle persone autorizzate ad accedere ai dati in questione: si tratta del " diritto di conoscerne ".
- indipendentemente dal tipo di supporto fisico, digitale o cartaceo, questi ultimi devono essere protetti. Occorre essere particolarmente vigili riguardo le attrezzature mobili e non lasciare senza sorveglianza o protezione tali attrezzature.

Per qualsiasi domanda, rivolgersi al Responsabile della Sicurezza dei Sistemi informativi del gruppo Elior.

E. Subappalto e trasferimento di dati personali

In caso di trasferimento di dati personali, il gruppo Elior deve innanzitutto accertarsi che quest'ultimo sia legalmente possibile e protetto. Il trasferimento di dati personali deve essere interpretato in senso ampio; può, ad esempio, trattarsi di:

- trasferimenti di dati tra entità giuridiche all'interno del gruppo Elior;
- una gestione o manutenzione esternalizzata di una risorsa informatica;
- l'hosting di un servizio nel cloud.

Obblighi del Responsabile

Conformemente al GDPR, il subappaltatore è tenuto ad accompagnare il titolare del trattamento nel suo intervento permanente di messa in conformità. Il titolare del trattamento è tenuto a garantire che il subappaltatore assolva tale compito. Il subappaltatore è tenuto a un obbligo di:

- **trasparenza**: resa possibile dalla stesura di un atto legale (i) che definisca chiaramente gli obblighi di ciascuna delle parti, (ii) precisando che il subappaltatore opera esclusivamente dietro istruzioni del titolare del trattamento. Tale trasparenza è garantita anche mantenendo un registro aggiornato delle attività svolte per conto del titolare del trattamento e mettendo a disposizione tutte le informazioni necessarie per dimostrare il rispetto di tali obblighi;
- **consulenza e assistenza**: il subappaltatore deve assistere il titolare del trattamento nella determinazione dei dati strettamente necessari, nel trattamento delle richieste di esercizio dei diritti e, più in generale, per l'adempimento di tutti i suoi obblighi;
- **sicurezza**: il subappaltatore deve accertarsi che i propri dipendenti siano soggetti a un obbligo di riservatezza e deve adottare ogni misura volta a garantire un livello di sicurezza adeguato ai rischi e una conservazione dei dati per la stretta durata prevista;
- **notifica**: il subappaltatore deve notificare al titolare del trattamento ogni violazione di dati entro un termine ragionevole (idealmente 24 o 36 ore).

Il gruppo Elior e i suoi team si impegnano ad accertarsi del rispetto di tali requisiti per ogni ricorso a subappaltatori e quando il gruppo Elior agisce in qualità di subappaltatore.

Laddove il gruppo Elior agisca in qualità di titolare del trattamento e si avvalga di uno o più subappaltatori, il o i subappaltatori devono ottemperare alle esigenze del gruppo Elior in materia di protezione dei dati personali. Il trasferimento di dati a subappaltatori deve avvenire in modo protetto. È responsabilità del gruppo Elior accertarsi che i suoi subappaltatori abbiano adottato misure adeguate per garantire la sicurezza dei dati personali.

Le direzioni legali devono essere consultate sistematicamente per verificare che tutti i contratti prevedano gli obblighi in materia di protezione dei dati personali.

Caso particolare dei trasferimenti al di fuori dello Spazio Economico Europeo (SEE)

Il trasferimento di dati personali al di fuori dello SEE deve essere disciplinato da meccanismi appropriati, ad esempio:

- la firma delle clausole contrattuali standard approvate dalla Commissione europea;
- l'elaborazione di regole aziendali vincolanti: BCR per « titolare del trattamento » o BCR per « subappaltatore »;
- la sottoscrizione di impegni specifici (es. Privacy Shield) per gli organismi con sede al di fuori dello SEE.

F. Esercizio dei diritti

Il gruppo Elior ha cura che gli interessati possano godere pienamente dei loro diritto, in particolare:

- accedere ai dati personali che li riguardano;
- chiedere la rettifica dei dati personali che li riguardano;
- chiedere la portabilità dei dati personali che li riguardano in un formato strutturato;
- opporsi ad essere oggetto di una decisione fondata esclusivamente su un trattamento automatizzato;
- chiedere la cancellazione dei dati personali;
- chiedere la limitazione del trattamento dei dati personali;
- opporsi al trattamento dei dati personali.

G. Privacy by design

E' più semplice e meno costoso tener conto quanto prima nei progetti delle considerazioni in materia di privacy e sicurezza. Per questo, all'avvio di un nuovo progetto, il responsabile del progetto deve prendere in considerazione la problematica della protezione dei dati personali e garantire il rispetto della privacy degli interessati, sia nell'attuazione di un nuovo servizio/prodotto che durante la sua modifica.

Ciò significa, in particolare, che il responsabile del progetto deve:

- identificare i dati personali che potrebbero essere presenti;
- se applicabile:
    - inserire questo progetto nell'ambito dello strumento di gestione della protezione dei dati personali e seguire le indicazioni,
    - identificare i principali rischi legati ai dati personali che possono verificarsi nell'ambito di un particolare progetto, in particolare i rischi giuridici, i rischi legati alla reputazione e i rischi per le persone,
    - per il trattamento dii dati ad alto rischio, effettuare una valutazione d'impatto sulla protezione dei dati (« DPIA"). Tali trattamenti riguardano in particolare l'utilizzo di dati su vasta scala, l'uso di nuove tecnologie, l'elaborazione di dati sensibili, la sorveglianza sistematica o l'implementazione di un trattamento per il processo decisionale automatizzato e il profiling. Il Comitato europeo per la protezione dei dati propone sul suo sito, paese per paese, l'elenco dei trattamenti per i quali è obbligatorio un DPIA,
    - accertarsi della conformità alla politica del Gruppo,
    - garantire l'attuazione e il controllo dei meccanismi di protezione organizzativi e tecnici.

In caso di necessità di supporto o di precisazioni, il responsabile del progetto può rivolgersi ai suoi ambasciatori DCP.

H. Comunicazione e sensibilizzazione

Su base annuale, in funzione delle sfide individuate e delle constatazioni relative alla conformità del gruppo Elior, il team Gruppo avvia un piano di comunicazione e di sensibilizzazione, con il supporto degli ambasciatori DCP. Tale approccio deve avere l'obiettivo di instaurare una cultura della protezione dei dati personali all'interno del gruppo Elior.

I team sono invitati a contribuire al miglioramento della politica e dei processi associati.

I. Categorie particolari di trattamenti e di dati personali

Dati personali sensibili o assimilati

Si tratta di informazioni che rivelano le origini razziali o etniche, le opinioni politiche, filosofiche o religiose, l'appartenenza sindacale, la salute o la vita sessuale di una persona fisica. Anche le informazioni relative ai reati e alle condanne devono essere considerate tali.

Si raccomanda all'interno del gruppo Elior di non raccogliere o utilizzare tali dati a causa degli elevati rischi per la privacy delle persone, salvo in casi specifici:

- se l'interessato ha dato il suo espresso consenso (scritto, chiaro ed esplicito);
- se tali dati sono necessari per scopi medici o per la ricerca in campo sanitario ;
- se il loro utilizzo è autorizzato dall'autorità preposta alla protezione dei dati personali.

Questi casi possono variare in base al diritto nazionale del paese; per questo tipo di problematiche è quindi opportuno contattare gli ambasciatori DCP o il team RGPD Gruppo. Si dovrà sistematicamente realizzare una DPIA.

Dati personali e diritto all'immagine relativi ai bambini

I bambini meritano una protezione specifica per quanto riguarda i loro dati personali in quanto possono essere meno consapevoli dei rischi, delle conseguenze o delle garanzie che devono essere fornite e dei loro diritti relativi al trattamento dei dati personali.

Nell'ambito dei servizi della società dell'informazione, il trattamento dei dati personali relativi a un bambino è lecito quando il soggetto ha almeno 16 anni. Quando il soggetto ha meno di 16 anni, questo trattamento è lecito solo se e nella misura in cui il consenso è dato o autorizzato dal titolare della responsabilità parentale nei confronti del bambino. Gli Stati membri possono prevedere per legge un'età inferiore per tali scopi, a condizione che tale età non sia inferiore a 13 anni. Si invita a contattare l'ambasciatore DCP per identificare la soglia d'età in funzione del trattamento previsto.

Prima dell'attuazione di questi trattamenti si dovrà sistematicamente realizzare una DPIA.

Operazioni marketing

Le operazioni di marketing devono rispettare le scelte e i diritti degli interessati. In occasione delle operazioni di marketing, in particolare per via elettronica, occorre accertarsi che:

- gli interessati abbiano dato il loro esplicito consenso (per i rapporti BtoC);
- le persone non abbiano esercitato il diritto di opposizione alla prospezione;
- i messaggi offrano la possibilità di annullare facilmente l'abbonamento ("opt-out");
- nessun destinatario possa vedere i nomi e i dati degli altri destinatari.

J. Violazioni dei dati

Nonostante l'applicazione di standard di alto livello per garantire la sicurezza dei dati, il gruppo Elior non può tutelarsi totalmente dal rischio di violazioni di dati che possono essere configurarsi in:

- una violazione della riservatezza, vale a dire una fuga di dati (es. perdita di chiavetta USB contenente file clienti);
- una violazione dell'integrità, ossia una modifica non prevista (es. modifica non desiderata del database che indica automaticamente alle autorità l'assegnatario di un'auto aziendale);
- un attacco alla disponibilità, vale a dire la distruzione di dati (es. software malevolo che cifra un database).

La fonte di tali violazioni può essere sia esterna (es. attacco a una risorsa del gruppo Elior o a un provider esposto a Internet) che interna. Può anche essere intenzionale o accidentale (es. schermo non protetto da filtro di riservatezza esposto nei trasporti pubblici).

È responsabilità di ognuno vigilare e segnalare immediatamente qualsiasi violazione dei dati al team RGPD Gruppo. In caso di violazione, accertata o presunta, della sicurezza, occorre agire immediatamente per limitare gli effetti e i danni. Nei casi più gravi, il gruppo Elior dovrà informare l'autorità preposta alla protezione dei dati e fornirle un piano d'azione che consenta di mitigare gli impatti della violazione entro 72 ore e, in alcuni casi, informare anche gli interessati.

K. Controllo e relazione con le autorità preposte alla protezione dati

Potenziali impatti della mancata considerazione della protezione dei dati personali

Le violazioni della normativa sulla protezione dei dati personali possono avere gravi conseguenze, in particolare:

- sanzioni finanziarie pari a sino il 4% del fatturato totale del gruppo Elior;
- richieste di indennizzo delle persone interessate dalla violazione della privacy ;
- messa in conformità con penalità, la limitazione di un trattamento o la sospensione dei flussi di dati;
- danno alla reputazione e all'immagine del gruppo Elior.

Potere delle autorità preposte alla protezione dei dati

Il gruppo Elior ha in corso di redazione il *Binding Corporate Rules*. Le BCR hanno l'obiettivo di dimostrare il rispetto di un livello di protezione dei dati simile a prescindere dall'ubicazione dell'entità giuridica controllata del gruppo Elior e di autorizzare i trasferimenti di dati personali all'interno del gruppo Elior.

L'autorità preposta alla protezione dei dati personali dispone del potere di controllare la conformità al Regolamento generale sulla protezione dei dati attraverso controlli fisici o a distanza e, in particolare, può:

- ottenere copia del massimo di informazioni, tecniche e giuridiche, per valutare le condizioni in cui vengono effettuati trattamenti di dati personali;
- chiedere che le vengano trasmessi tutti i documenti necessari per lo svolgimento della propria missione;
- accedere ai programmi informatici e ai dati e richiederne la trascrizione;
- richiedere copia di contratti (es. contratti di locazione di file, contratti di subappalto informatico), moduli, fascicoli cartacei, database, ecc.
- realizzare a distanza scansioni di vulnerabilità, audit di sicurezza e verificare la presenza delle informazioni legali.

In Francia, l'articolo 51 della legge francese n. 78-17 del 6 gennaio 1978 e successive modifiche, relativa all'informatica, ai file e alle libertà detta "loi Informatique et Libertés" stabilisce che qualsiasi impedimento all'azione della Cnil è punibile con un anno di detenzione e €15.000 di ammenda. L'impedimento all'azione dell'autorità preposta alla protezione dei dati personali viene realizzato in caso di:

- opposizione all'esercizio dei compiti affidati ai membri o agli agenti autorizzati quando la visita è stata autorizzata dal giudice delle libertà e della detenzione;
- rifiuto di comunicare, nascondere o distruggere informazioni e documenti utili all'incarico di controllo;
- comunicazione di informazioni non conformi al contenuto delle registrazioni, così come era nel momento in cui è stata formulata la richiesta dell'autorità preposta alla protezione dei dati personali o di presentazione di un contenuto in una forma non direttamente accessibile.

Gestione:

Si raccomanda di contattare immediatamente il team Gruppo e di cooperare pienamente con le autorità dopo la verifica dell'identità delle persone (mandato e carta d'identità professionale).

Il team Gruppo è l'unica entità autorizzata a comunicare con le autorità preposte alla protezione dei dati (es.: approccio preliminare, richiesta di informazioni, risposta alle procedure di deferimento, ecc.). Qualsiasi richiesta da parte delle autorità deve quindi essere immediatamente notificata.

5. Informazioni aggiuntive

Per eventuali domande riguardo questa politica o ulteriori informazioni su uno o più degli argomenti trattati, contattare il team Gruppo al seguente indirizzo e-mail: gdpr-contact@eliorgroup.com.