Direttiva di BMS Building Materials Suisse in materia di protezione dei dati

in conformità con il Regolamento generale sulla protezione dei dati dell'UE e con la Legge svizzera sulla protezione dei dati

Reparto:	Legal & Compliance
Autori:	Christina Hooker, Legal Counsel
Data di creazione:	settembre 2022

La presente direttiva sulla protezione dei dati contiene disposizioni sulla protezione dei dati personali che si applicano a tutte le società del marchio ombrello BMS Building Materials Suisse (**aziende BMS**). Essa definisce l'importanza e il significato della protezione dei dati in termini di rispetto dei diritti e delle libertà fondamentali dei collaboratori, dei clienti e dei partner commerciali delle aziende BMS.

La presente direttiva sulla protezione dei dati si basa sul regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 sulla protezione delle persone fisiche nell'ambito del trattamento dei dati personali, sulla libera circolazione di tali dati e sull'abrogazione della direttiva 95/46/CE, sul Regolamento generale sulla protezione dei dati (**RGPD**) e sulla Legge federale svizzera, compresi i regolamenti sulla protezione dei dati (**LPD**).

Il RGPD, entrato direttamente in vigore in tutti gli Stati membri dell'Unione europea il 25 maggio 2018, contiene disposizioni sulla tutela delle persone fisiche- con riguardo al trattamento dei dati personali e sulla libera circolazione di tali dati nel mercato interno europeo, nonché sulla tutela dei diritti e delle libertà fondamentali delle persone fisiche e, in particolare, del loro diritto alla protezione dei dati personali (art. 1 RGPD).

Ai sensi dell'art. 3 cpv. 1 RGPD, il presente regolamento si applica al trattamento dei dati personali nella misura in cui esso è effettuato nel contesto delle attività di una filiale di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento abbia luogo nell'Unione. Poiché le aziende BMS sono società del Gruppo BME con sede legale nell'Unione e data la decisione di BME di implementare il RGPD a livello di gruppo, lo stesso si applica anche alle aziende BMS, che sono tenute a osservarne le disposizioni nel trattamento dei dati personali.

In quanto titolari di filiali in Svizzera, le aziende BMS sono ovviamente soggette anche alla Legge svizzera sulla protezione dei dati.

Cosa c'è da sapere

Il Regolamento generale sulla protezione dei dati e la Legge svizzera sulla protezione dei dati disciplinano le modalità di protezione dei dati personali quando questi vengono elaborati da terzi (persona o azienda).

Appartenendo a BME Building Materials Europe, gruppo con sede nei Paesi Bassi, ovvero all'interno dell'Unione europea, e intenzionato a implementare la protezione dei dati in modo omogeneo in tutte le sue aziende, siamo a nostra volta soggetti al RGPD, oltre che alla LPD svizzera in qualità di impresa elvetica.

Sommario

1. Oggetto

Oggetto della presente direttiva sulla protezione dei dati è il trattamento di dati personali interamente o parzialmente automatizzato, nonché il trattamento di dati personali non automatizzato, a prescindere dal tipo di trattamento e dalla forma (cartacea, digitale, verbale), purché i dati personali siano memorizzati o destinati a essere memorizzati in un sistema di archiviazione (cfr. art. 2 cpv. 1 RGPD art. 1 LPD).

2. Ambito di validità

La presente direttiva sulla protezione dei dati si applica a tutti i collaboratori delle aziende BMS incaricati del trattamento di dati personali.

Nell'ambito del loro contratto di lavoro, i collaboratori sono tenuti all'osservanza delle disposizioni pertinenti della legge sulla protezione dei dati e della presente direttiva sulla protezione dei dati. Le persone e le società esterne, nonché i partner commerciali incaricati del trattamento di gruppi di dati personali per conto di un'azienda BMS, sono contrattualmente obbligati a rispettare le disposizioni sulla protezione dei dati che li riguardano.

La presente direttiva sulla protezione dei dati disciplina anche il trattamento dei dati personali dei collaboratori delle aziende BMS. Tutti i collaboratori vengono informati circa le categorie dei loro dati personali elaborati dalle aziende BMS, le finalità del trattamento e i relativi diritti di cui dispongono in una comunicazione sulla protezione dei dati allegata al contratto di lavoro.

Cosa c'è da sapere

I dati personali sono: Informazioni che riguardano una persona vivente e che permettono di identificarla, come ad esempio nome e cognome, indirizzo, data di nascita, numero di telefono, numero di conto corrente, mansione lavorativa, foto, eventualmente anche indirizzi IP ecc.

Il termine trattamento indica: Qualsiasi procedura condotta su tali dati personali come la raccolta, la registrazione, l'organizzazione, la strutturazione, la memorizzazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, condivisione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la cancellazione o la distruzione.

La presente direttiva, oltre a tutelarti in quanto collaboratore di BMS, ti impone l'obbligo di salvaguardare i dati personali di terzi e contiene le regole da seguire per il trattamento dei dati di clienti, partner commerciali, fornitori, fornitori di servizi e visitatori del sito web.

3. Elenco delle attività di trattamento

Le aziende BMS hanno la responsabilità di tenere un registro delle attività di trattamento contenente almeno le seguenti informazioni:

a. il nome e i dati di contatto della rispettiva azienda BMS, oppure del rispettivo reparto responsabile
b. le finalità del trattamento
c. una descrizione delle categorie di interessati e delle categorie di dati personali
d. le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari in Paesi terzi
e. eventuali trasferimenti di dati personali verso un Paese terzo, con indicazione dello stesso
f. se possibile, i termini previsti per la cancellazione delle diverse categorie di dati
g. se possibile, una descrizione generale delle misure tecniche e organizzative ai sensi dell'art. 32 cpv. 1 RGPD, art. 11 LPD.

Cosa c'è da sapere

Teniamo un registro in cui elenchiamo tutte le procedure con cui vengono trattati i dati personali (dei nostri collaboratori, clienti, partner commerciali ecc.). Questo registro è importante perché ci permette di identificare i dati personali trattati con le relative misure di protezione adottate per il trattamento, nonché i responsabili della protezione all'interno dell'azienda e i dati personali effettivamente trattati. Questo elenco viene presentato anche in caso di controlli di due diligence da parte di un'autorità di vigilanza.

4. Principi per il trattamento di dati personali

Le aziende BMS effettuano il trattamento dei dati personali attenendosi ai seguenti principi:

- **liceità, trattamento in buona fede, trasparenza**
  I dati personali devono essere trattati in modo lecito, in buona fede e in una maniera che sia trasparente per l'interessato (cfr. art. 5 cpv. 1 lett. a RGPD, art. 4 cpv. 1, 2, 3 LPD).

- **Limitazione delle finalità**
  I dati personali devono essere raccolti per finalità specifiche, esplicite e legittime e non devono essere ulteriormente trattati in maniera incompatibile con le stesse (cfr. art. 5 cpv. 1 lett. b RGPD, art. 4 cpv. 3 LPD).

- **Minimizzazione dei dati**
  I dati personali devono essere adeguati e pertinenti allo scopo nonché limitati a quanto necessario per le finalità del trattamento (cfr. art. 5 cpv. 1 lett. c RGPD, art. 4 cpv. 3 LPD).

- **Esattezza**
  I dati personali devono essere corretti dal punto di vista fattuale e, se necessario, aggiornati (cfr. art. 5 cpv. 1 lett. d RGPD, art. 4 cpv. 5 LPD).

- **Limitazione della conservazione**
  I dati personali devono essere conservati in una forma che consenta l'identificazione degli interessati per un periodo di tempo non superiore a quello necessario per il conseguimento delle finalità per cui sono trattati (cfr. art. 5 cpv. 1 lett. e RGPD, art. 4 cpv. 4 LPD).

- **Integrità e riservatezza**
  I dati personali devono essere trattati in modo da garantirne la necessaria sicurezza, proteggendoli con misure tecniche e organizzative adeguate contro il trattamento non autorizzato o illegale e contro la perdita, la distruzione o il danneggiamento accidentali (cfr. art. 5 cpv. 1 lett. f RGPD).

- **Responsabilità**
  Le aziende BMS devono garantire ed essere in grado di dimostrare il rispetto dei principi sopra citati per tutti i dati personali (cfr. art. 5 cpv. 2 RGPD)

4.1 Liceità del trattamento

Le aziende BMS trattano i dati personali solo se almeno una delle condizioni di cui all'art. 6 cpv. 1 RGPD e all'art. 24 LPD è soddisfatta, in particolare:

- l'interessato ha fornito il **consenso** al trattamento dei propri dati personali per una o più finalità specifiche;

- il trattamento è necessario per l'**esecuzione di un contratto** di cui l'interessato è parte contrattuale o per l'attuazione di misure precontrattuali adottate su richiesta dell'interessato;

- il trattamento è necessario per l'**adempimento di un obbligo legale** a cui è soggetta la rispettiva azienda BMS;

- il trattamento è necessario per la **salvaguardia dei legittimi interessi dell'azienda BMS in questione** o di una terza parte, a meno che su tali interessi non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali. Ai sensi dell'art. 24 cpv. 2 LPD, gli interessi dell'azienda BMS in questione si intendono prevalenti in particolare
    - se detta azienda è o intende entrare in concorrenza economica con un'altra persona e tratta i dati personali a tale scopo senza divulgarli a terzi;
    - se i dati personali sono trattati per verificare la solvibilità dell'interessato (cliente) (e se non si tratta di dati personali che richiedono una protezione speciale, se vengono comunicati solo i dati necessari per la conclusione o l'esecuzione di un contratto con l'interessato e se l'interessato è maggiorenne).

4.2 Condizioni per il consenso

- La rispettiva azienda BMS ottiene per tempo il consenso necessario dagli interessati.
- Il consenso è espresso con un chiaro atto confermativo che dichiara come l'interessato acconsenta al trattamento dei dati personali che lo riguardano su base volontaria, per il caso specifico, in modo informato e inequivocabile.
- Il modulo della dichiarazione di consenso deve essere fornito in forma comprensibile e facilmente accessibile nonché in un linguaggio chiaro e semplice. È chiaramente distinguibile da altre questioni e non contiene clausole abusive.
- Inoltre, l'interessato dispone di un metodo semplice per revocare il consenso in qualsiasi momento.

4.3 Requisiti per la definizione delle finalità

- I dati personali devono essere raccolti per finalità specifiche, esplicite e legittime e non devono essere ulteriormente trattati in maniera incompatibile con le stesse.
- In determinate circostanze, i dati personali possono essere trattati per finalità aggiuntive rispetto a quelle originariamente previste al momento della raccolta, che devono essere inserite nel registro e, se necessario, comunicate agli interessati.

4.4 Trattamento dei dati personali di minori

- In linea di principio, le aziende BMS trattano i dati personali solo di minori che abbiano compiuto il sedicesimo anno di età.
- In tutti gli altri casi, il trattamento ha luogo solo nelle modalità e nei limiti previsti dal relativo consenso fornito dal titolare della responsabilità genitoriale del minore.

4.5 Trattamento di particolari categorie di dati personali

- Il trattamento di dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché il trattamento di dati genetici, di dati biometrici intesi a identificare in modo univoco una persona fisica, di dati relativi alla salute o di dati relativi alla vita sessuale o all'orientamento sessuale di una persona fisica o di dati relativi a procedimenti amministrativi o penali e a sanzioni, è in linea di principio vietato in assenza di un consenso esplicito (art. 9 cpv. 1 RGPD, art. 4 cpv. 6 LPD).
- Le aziende BMS trattano, tutt'al più, categorie particolari di dati personali esclusivamente dei collaboratori e solo nel quadro dell'organizzazione delle attività aziendali nonché per adempiere e verificare gli obblighi previsti dalla normativa sul lavoro e sulla previdenza sociale. Il trattamento di questa categoria di dati personali è subordinato al consenso esplicito dell'interessato, in assenza di un altro motivo di giustificazione.

4.6 Marketing digitale

- Le aziende BMS non inviano comunicazioni a scopo pubblicitario o di marketing ai contatti attraverso mezzi digitali come la telefonia mobile, la posta elettronica o Internet senza aver ottenuto il consenso degli interessati.
- In presenza del consenso al trattamento dei dati personali per finalità di marketing digitale, al momento della prima raccolta dei dati l'interessato viene informato del proprio diritto di revocare in qualsiasi momento il trattamento dei suoi dati personali per detti scopi.

4.7 Periodo di conservazione

- Le aziende BMS non conservano i dati personali per un periodo superiore a quello necessario per gli scopi per i quali sono stati originariamente raccolti o successivamente trattati (cfr. art. 5 cpv. 1 lett. e RGPD, art. 4, cpv. 4 LPD).
- Il concetto di necessità dipende dalle circostanze del singolo caso, in considerazione dei motivi per cui i dati personali sono stati raccolti.

Cosa c'è da sapere

Ci atteniamo ai principi del RGPD e della LPD: trattiamo i dati personali in modo **lecito,** solo per **scopi chiaramente definiti** (e non oltre), solo **la quantità** di dati personali **strettamente necessaria,** solo i dati personali **corretti, conserviamo** i dati personali **solo per il tempo necessario** e li **proteggiamo** al meglio da perdita, distruzione, danneggiamento e diffusione illegale.

I dati personali si considerano trattati in modo lecito se il trattamento è dettato da un **elemento giuridico valido** (RGPD) o ha un **motivo di giustificazione** (LPD), in particolare se i dati personali sono trattati per **adempiere** un **contratto** o un **obbligo legale,** per **soddisfare i nostri legittimi interessi economici** (a condizione che questi prevalgano sui diritti e le libertà fondamentali dell'interessato) o se abbiamo ottenuto il **consenso** dell'interessato dopo averlo chiaramente informato del trattamento dei suoi dati personali. Il consenso deve essere ottenuto soprattutto per il trattamento nel contesto di misure di marketing.

Affinché il **consenso sia valido,** devi:

- ottenerlo in tempo utile;
- assicurarti che sia inequivocabile e venga fornito per un caso concreto. Ad esempio, sotto i campi per l'inserimento dei dati personali per l'iscrizione a una newsletter deve essere presente uno strumento con cui esprimere il proprio consenso, nella forma di una casella da selezionare in modo proattivo e che non contenga già un segno di spunta;
- assicurarti che il modulo di consenso sia chiaro e di facile comprensione, in modo che l'interessato sia davvero adeguatamente informato prima di fornire il proprio consenso;
- offrire la possibilità di ritirare il consenso in qualsiasi momento. Ad esempio, ogni newsletter deve contenere un'opzione che permetta di cancellare l'iscrizione con 1 o 2 clic del mouse.

Per il trattamento dei dati personali degli apprendisti di età inferiore a 17 anni, è necessario ottenere il consenso informato dei genitori.

I dati personali particolarmente sensibili vengono trattati solo dal reparto HR. Essi sono pertanto anche oggetto di una protezione particolare da parte dei collaboratori del reparto HR, in possesso della necessaria formazione.

5. Diritti degli interessati

I titolari dei dati personali sottoposti a trattamento dispongono di determinati diritti ai sensi del RGPD e della LPD.

5.1 Obbligo di informazione

Al momento della raccolta dei dati personali, la rispettiva azienda BMS comunica all'interessato quanto segue (cfr. art. 13 cpv. 1 RGPD, art. 19 LPD): Il proprio **nome** e i propri **dati di contatto,** le **finalità** del trattamento dei dati personali e la **base giuridica** del trattamento o, eventualmente, i **legittimi interessi** perseguiti dal responsabile del trattamento o da una terza parte (solo ai sensi del RGPD), se del caso i **destinatari** dei dati personali e l'eventuale intenzione di trasferire i dati personali in un **Paese terzo.** La LPD svizzera prevede che, in caso di divulgazione dei dati personali all'estero, la rispettiva azienda comunichi agli interessati anche il **Paese ed eventuali garanzie** (per la protezione dei dati personali all'estero).

Inoltre, al momento della raccolta di tali dati, la rispettiva azienda BMS fornisce all'interessato le seguenti ulteriori informazioni, necessarie a garantire un trattamento equo e trasparente: Il **periodo di conservazione** o, qualora non sia possibile, i criteri per determinare il periodo di conservazione, l'esistenza di un **diritto all'informazione,** alla **rettifica** e alla **cancellazione,** alla **limitazione del trattamento** e all'**opposizione** e, laddove il consenso sia stato ottenuto, il diritto di **revocare il consenso in qualsiasi momento** (senza pregiudicare la liceità del trattamento effettuato sulla base del consenso fino alla revoca) nonché l'esistenza di un **diritto di ricorso** all'autorità di controllo.

5.2 Diritti di informazione

Tutti gli interessati i cui dati sono sottoposti a trattamento dalle aziende BMS hanno il diritto, previa richiesta scritta via e-mail all'indirizzo **dataprotection@bmsuisse.ch** e verifica della loro identità, di richiedere alla rispettiva azienda BMS la conferma di un eventuale trattamento dei loro dati personali. In tal caso, l'interessato ha il diritto di ricevere tutte le informazioni di cui all'art. 15 cpv. 1 RGPD, art. 25 LPD in relazione ai propri dati personali, ovvero:

- identità e dati di contatto della nostra azienda;
- finalità del trattamento;
- categorie dei dati personali;
- destinatari a cui sono stati comunicati i dati personali, in particolare nel caso di destinatari in Paesi terzi;
- informazioni sulle esportazioni, tra cui un elenco dei Paesi e la base giuridica (solo ai sensi della LPD svizzera);
- se possibile, la durata prevista per la conservazione dei dati personali o i criteri per la definizione di tale periodo;
- l'esistenza di un diritto alla rettifica o alla cancellazione dei dati personali che lo riguardano o alla limitazione del trattamento da parte della rispettiva azienda BMS o di un diritto di opporsi a tale trattamento;

- l’esistenza di un diritto di ricorso a un’autorità di controllo;
- tutte le informazioni disponibili sull’origine dei dati, qualora gli stessi non vengano raccolti presso l’interessato;
- laddove i dati personali vengano trasferiti a un Paese terzo con l’obbligo di fornire garanzie adeguate al riguardo, l’interessato ha il diritto di essere informato di tali garanzie.

In determinate circostanze, la divulgazione delle informazioni richieste all’interessato potrebbe comportare la comunicazione di dati personali di un altro interessato. In casi del genere, le informazioni in questione devono essere modificate o ridotte, come ritenuto necessario o appropriato per proteggere i diritti della persona in questione.

Ai sensi della LPD svizzera, le aziende BMS possono rifiutare, limitare o differire la divulgazione se:

- una legge lo prevede in senso formale, ovvero per proteggere un segreto professionale;
- ciò è necessario a causa di interessi prevalenti di terzi; o
- la richiesta di informazioni è manifestamente infondata, ovvero persegue uno scopo contrario alla protezione dei dati o è chiaramente ostativa.

Le richieste di informazioni da parte degli interessati vengono elaborate in conformità alla **procedura** e presentate a dataprotection@bmsuisse.ch tramite l’apposito **modulo**.

5.3 Profilazione/decisioni automatizzate in casi individuali

Le aziende BMS ricorrono alla profilazione solo nell’attuale strumento HRIS di BMS. La profilazione viene effettuata con il consenso esplicito degli interessati o per l’esecuzione di contratti tra gli interessati e le aziende BMS, con l’adozione di misure appropriate per proteggere i diritti e le libertà nonché i legittimi interessi degli interessati.

5.4 Diritto di rettifica

L'interessato ha facoltà di richiedere la rettifica dei dati personali che lo riguardano alla rispettiva azienda BMS. Ciò include il diritto di richiedere il completamento/l'integrazione di dati personali incompleti (tenendo conto delle finalità del trattamento). Le richieste vengono elaborate in conformità alla procedura e presentate a dataprotection@bmsuisse.ch tramite l'apposito modulo.

5.5 Diritto di cancellazione

Gli interessati hanno il diritto, a determinate condizioni, di richiedere alla rispettiva azienda BMS la cancellazione dei dati personali che li riguardano (l'anonimizzazione irrevocabile è equivalente alla cancellazione) e la rispettiva azienda è obbligata a cancellare/anonimizzare irrevocabilmente i dati personali, in presenza di uno dei seguenti motivi (cfr. art. 17 cpv. 1 RGPD, art. 32 cpv. 2 lett. c LPD):

- i dati personali non sono più necessari per le finalità per cui sono stati raccolti;
- l'interessato revoca il consenso e non esiste un'altra base giuridica per il trattamento;
- l'interessato si oppone al trattamento e non sussistono motivi legittimi per effettuarlo comunque;
- i dati personali sono stati trattati illegalmente;
- la cancellazione dei dati personali è richiesta dalla legge svizzera.

Il diritto alla cancellazione dei dati personali non sussiste laddove il trattamento sia necessario:

- per l'esercizio del diritto alla libertà di espressione e di informazione;
- per adempiere un obbligo legale o per svolgere un compito di interesse pubblico o nell'esercizio di poteri ufficiali conferiti alla rispettiva azienda BMS;
- per l'affermazione, l'esercizio o la difesa di rivendicazioni legali.

Le richieste di cancellazione vengono elaborate in conformità alla procedura e presentate a dataprotection@bmsuisse.ch tramite l'apposito modulo.

Cosa c'è da sapere

Ogni soggetto interessato dal trattamento dei propri dati personali ha i seguenti **diritti:**

- il diritto di ricevere informazioni corrette e complete, in particolare: sul trattamento e sull'incaricato del trattamento, su tutti i diritti esistenti, sull'estensione della finalità del trattamento e sulla possibilità di revocare il consenso in qualsiasi momento;
- il diritto, in qualità di interessato, di ricevere informazioni su un eventuale trattamento e, in tal caso, di quali dati e con quali modalità;
- il diritto di far rettificare o integrare dati personali errati o incompleti;
- il diritto alla cancellazione dei dati personali se
    - non sono più necessari;
    - non è più presente alcun consenso;
    - è stata presentata opposizione al trattamento;
    - il trattamento era illegale;
    - una legge svizzera prevede la cancellazione.

I link a procedure e moduli sono riportati nel capitolo precedente.

I moduli per le richieste di informazioni, rettifica/modifica e cancellazione debitamente compilati vanno inviati all'indirizzo dataprotection@bmsuisse.ch.

6. Trasmissione di dati personali a terzi

6.1 Principio

Il trasferimento dei dati personali a un Paese terzo può essere effettuato se il Paese terzo in questione garantisce un livello di protezione adeguato. Tale trasmissione di dati non richiede un'autorizzazione particolare (cfr. art. 45 RGPD, art. 16 f LPD).

In assenza di una decisione di adeguatezza da parte della Commissione, le aziende BMS possono trasferire dati personali a un Paese terzo solo dopo aver fornito garanzie adeguate nonché assicurato diritti applicabili e mezzi di ricorso efficaci agli interessati (cfr. art. 46 RGPD, art. 16 cpv. 2 LPD).

In mancanza sia di una decisione di adeguatezza che di garanzie appropriate, le aziende BMS trasferiscono i dati personali a un Paese terzo solo in presenza di determinate condizioni, le più importanti delle quali sono:

- l'interessato ha fornito il suo consenso esplicito al trasferimento dei dati dopo essere stato informato dei possibili rischi che comporta l'assenza di una decisione di adeguatezza e di garanzie appropriate;
- il trasferimento è necessario per l'esecuzione di un contratto tra l'interessato e la rispettiva azienda BMS o per l'attuazione di misure precontrattuali su richiesta dell'interessato.

6.2 Trasmissioni tra BMS e BME o altre aziende all'interno di BME

L'efficiente svolgimento delle attività commerciali delle aziende BMS può richiedere il trasferimento dei dati personali a BME o ad altre aziende facenti capo a BME o la concessione dell'accesso ai dati personali da parte di BME. In particolare, i dossier dei collaboratori di BMS possono essere trasferiti al reparto del personale di BME ad Amsterdam ai fini della retribuzione dei dirigenti e dello sviluppo/della formazione del personale, adottando sempre le misure necessarie a proteggere i dati personali.

Se l'azienda destinataria dei dati si trova in un Paese terzo, la rispettiva azienda BMS utilizza meccanismi di trasmissione in grado di garantire agli interessati diritti vincolanti e applicabili in relazione al trattamento dei loro dati personali (clausole tipo di protezione dei dati) o richiede il consenso espresso al trasferimento dell'interessato debitamente informato.

In particolare, le aziende BMS e i loro collaboratori si assicurano

- di ottenere l'autorizzazione del reparto Legal & Compliance prima del trasferimento a un Paese terzo;
- che venga trasmessa solo la quantità minima di dati personali necessaria allo scopo del trasferimento;
- che siano adottate misure di sicurezza adeguate per proteggere i dati personali durante la trasmissione.

6.3 Trasferimenti ad altri soggetti terzi

Le aziende BMS trasferiscono i dati personali a terzi e concedono l'accesso ai dati personali a terzi solo laddove siano garantiti la legalità del loro trattamento e un livello di protezione adeguato da parte del destinatario.

Nel caso in cui i dati personali siano trattati da un soggetto terzo, la rispettiva azienda BMS deve innanzitutto chiarire se, in conformità alla legge applicabile, tale terzo occupa la posizione di responsabile o di incaricato del trattamento dei dati personali in questione.

Qualora il soggetto terzo sia il responsabile del trattamento dei dati, la rispettiva azienda BMS stipula un accordo congiunto con lo stesso, per definire le responsabilità di ciascuna parte in relazione ai dati personali trasferiti.

Se il soggetto terzo è invece l'incaricato del trattamento, la rispettiva azienda BMS stipula con lui un contratto di trattamento dei dati, in cui lo obbliga a rispettare i principi della legge sulla protezione dei dati (cfr. art. 28 RGPD, art. 9 LPD).

In determinate circostanze, è consentito divulgare i dati personali senza che l'interessato ne sia a conoscenza o abbia fornito il proprio consenso, ad esempio quando ciò è necessario ai fini di prevenzione, indagine, accertamento o perseguimento di reati o dell'esecuzione di sanzioni penali.

Cosa c'è da sapere

I dati personali possono anche essere inviati in un altro Paese e lì trattati. Tuttavia, questo Paese deve avere leggi che garantiscano un'adeguata protezione dei dati personali inviati. Tutti i Paesi dell'Unione europea soddisfano questo requisito, in quanto soggetti al RGPD. Anche la Svizzera e il Regno Unito, ad esempio, hanno leggi che garantiscono una protezione adeguata e il trasferimento di dati a questi Paesi non richiede un'autorizzazione speciale.

Questo vale anche per l'invio di dati personali alla nostra società madre BME. Naturalmente, i contratti sul trattamento dei dati o gli accordi per il trasferimento dei dati vengono sottoscritti anche quando i dati vengono trasmessi a un cosiddetto Paese sicuro, garantendo che i dati personali siano adeguatamente protetti durante il trasferimento e il trattamento, ma senza la necessità di ulteriori misure.

Gli Stati Uniti e alcuni altri Paesi, invece, non possono garantire un'adeguata protezione dei dati personali e, nel loro caso, è richiesta un'autorizzazione separata. Il più delle volte questa è rappresentata dal consenso esplicito della persona interessata (informata in anticipo e con chiarezza del trasferimento e/o trattamento dei suoi dati personali in un Paese non sicuro) oppure, qualora si tratti dei dati personali di più persone, dalla stipula di cosiddette clausole tipo di protezione dei dati, che garantiscono misure di protezione aggiuntive.

L'adeguata protezione dei dati personali da noi condivisi con fornitori di servizi (logistica, IT ecc.), fornitori, partner commerciali e altri soggetti terzi è da noi garantita tramite contratti con gli incaricati del trattamento.

7. Misure tecniche e organizzative

Le aziende BMS adottano misure tecniche e organizzative adeguate per garantire la sicurezza dei dati personali in conformità con le normative vigenti in materia di protezione dei dati. Le rispettive misure adottate vengono annotate nel registro in corrispondenza del relativo trattamento.

8. Protezione dei dati mediante strumenti tecnici e attraverso impostazioni predefinite (privacy by design e privacy by default)

In considerazione dello stato dell'arte, dei costi di attuazione e della natura, dell'ambito, del contesto e delle finalità del trattamento, nonché della diversa probabilità e gravità dei rischi per i diritti e le libertà delle persone fisiche legati al trattamento, le aziende BMS adottano misure tecniche e organizzative adeguate sia al momento di determinare i mezzi per il trattamento sia al momento del trattamento effettivo (come la pseudonimizzazione), progettate per attuare efficacemente i principi di protezione dei dati di cui al capitolo 4 della presente direttiva sulla protezione dei dati e per incorporare nel trattamento le garanzie necessarie a tutelare i diritti degli interessati (art. 25 cpv. 1 RGPD, art. 7 LPD).

Le aziende BMS adottano misure tecniche e organizzative adeguate per garantire, in linea di principio e tramite impostazioni predefinite, che gli unici dati personali trattati siano quelli necessari alle finalità del trattamento stesso. Queste misure riguardano la quantità di dati personali raccolti, l'ambito del loro trattamento, il periodo di conservazione e l'accessibilità, in particolare impedendo l'accesso ai dati personali da parte di un numero indefinito di persone fisiche attraverso impostazioni predefinite (art. 25 cpv. 2 RGPD, art. 7 cpv. 3 LPD).

Per garantire che tutti i principi di protezione dei dati siano presi in considerazione nelle fasi di sviluppo, modifica o estensione di sistemi o processi, gli stessi devono essere sottoposti a una procedura di approvazione prima del loro (ulteriore) utilizzo. Per tutti i sistemi o processi nuovi o modificati viene inoltre effettuata una valutazione d'impatto sulla protezione dei dati, come definito nel capitolo 10 della presente direttiva sulla protezione dei dati.

9. Sensibilizzazione e formazione dei collaboratori

Le aziende BMS implementano processi e meccanismi interni adeguati per coinvolgere e sensibilizzare i collaboratori.

Tutti i collaboratori delle aziende BMS che hanno accesso ai dati personali ne condividono la responsabilità, ai sensi della presente direttiva sulla protezione dei dati. Nella fase di inserimento professionale vengono informati sulla direttiva sulla protezione dei dati personali, che si impegnano a rispettare. Le aziende BMS supportano i loro collaboratori nei processi pertinenti, organizzando inoltre corsi di formazione sulla protezione dei dati con almeno i seguenti contenuti:

a) i principi del trattamento dei dati personali, come indicati nel capitolo 4 della presente direttiva;
b) la responsabilità di ogni collaboratore nel garantire che i dati personali siano trattati solo da persone autorizzate e per scopi autorizzati;

c) a necessità e la corretta applicazione dei moduli e dei processi approvati per l'attuazione della presente direttiva sulla protezione dei dati;

d) l'uso corretto di password, token di sicurezza e altri meccanismi di accesso;

e) l'importanza di limitare l'accesso ai dati personali, ad esempio con screensaver protetti da password ed effettuando il logout;

f) conservazione sicura di atti fisici e supporti elettronici;

g) la necessità della relativa autorizzazione e di misure di sicurezza adeguate per tutti i trasferimenti di dati personali al di fuori della rete interna e dei locali aziendali;

h) il corretto smaltimento dei dati personali;

i) i rischi specifici relativi ai dati personali nel contesto delle attività o dei compiti di un reparto.

In caso di dubbi sul trattamento o sulla trasmissione dei dati personali, i collaboratori possono contattare il reparto Legal & Compliance all'indirizzo dataprotection@bmsuisse.ch.

Cosa c'è da sapere

Ci serviamo di misure tecniche e organizzative per proteggere i dati personali dei nostri collaboratori, clienti e partner commerciali.

Il nostro reparto IT, principale responsabile delle **misure tecniche,** garantisce il mantenimento di un elevato livello tecnologico, la protezione da attacchi esterni e interni, la visualizzazione/condivisione dei soli dati personali realmente necessari e la cancellazione di quelli non più necessari.

Per garantire che il nostro livello di protezione rimanga elevato, le nuove modalità di trattamento vengono esaminate mediante una valutazione d'impatto sulla protezione dei dati, in parallelo allo studio delle misure di protezione necessarie.

Tutti i collaborativi sono responsabili delle **misure organizzative** nonché tenuti al rispetto della disposizione ITC: si tratta di misure come il blocco dello schermo del computer, la chiusura a chiave degli schedari, la scelta di una password forte, ma anche la sensibilizzazione e la formazione dei collaboratori che trattano i dati personali.

Per maggiori informazioni sulle misure tecniche e organizzative o sui corsi di formazione offerti, è possibile rivolgersi a dataprotection@bmsuisse.ch.

10. Valutazione d'impatto sulla protezione dei dati

La rispettiva azienda BMS effettua preventivamente una valutazione d'impatto delle procedure di trattamento previste qualora la loro natura, a causa di modalità, portata, circostanze e finalità, possa comportare un rischio elevato per i diritti e le libertà degli interessati (art. 35, cpv. 1 RGPD, art. 22 LPD).

La valutazione d'impatto sulla protezione dei dati deve includere almeno i seguenti contenuti (cfr. art. 35 cpv. 7 RGPD, art. 22 cpv. 3 LPD):

a) una descrizione sistematica delle procedure di trattamento previste e delle finalità del trattamento;

b) una valutazione della necessità e della proporzionalità delle procedure di trattamento in relazione alla finalità;

c) una valutazione dei rischi per i diritti e le libertà degli interessati; e

d) le misure di mitigazione previste per la gestione dei rischi, comprese le garanzie, le misure di sicurezza e le procedure che assicurano la protezione dei dati personali e la dimostrazione della conformità al RGPD e alla LPD, tenendo conto dei diritti e degli interessi legittimi degli interessati e di altri soggetti interessati.

Ogni collaboratore responsabile dell'introduzione di una nuova procedura di trattamento (ad esempio per una nuova app o piattaforma, nuove videocamere, un nuovo e-shop ecc.), richiede il parere del reparto Legal & Compliance per decidere in merito alla necessità di una valutazione d'impatto sulla protezione dei dati. È necessario seguire le fasi previste dal **concetto per la valutazione d'impatto sulla protezione dei dati**.

11. Notifica della violazione di dati personali

In caso di violazione di dati personali di persone situate nell'Unione europea, il collaboratore che scopre la violazione o che ne riceve la relativa segnalazione deve innanzitutto comunicarla internamente a dataprotection@bmsuisse.ch subito dopo esserne venuto a conoscenza. A questo punto spetta al reparto Legal & Compliance decidere se la violazione dei dati personali può comportare un rischio elevato per i diritti e le libertà delle persone fisiche. In caso affermativo, lo stesso reparto segnala la violazione esternamente all'autorità di vigilanza competente (art. 33 cpv. 1 RGPD, art. 24 LPD).

La notifica deve contenere almeno le seguenti informazioni (art. 33 cpv. 3 RGPD, art. 24 cpv 2 LPD):

- descrizione della natura della violazione, comprese, laddove possibile, le categorie e il numero approssimativo delle serie di dati personali interessati;
- nome e recapiti del centro di contatto per ulteriori informazioni;

- descrizione delle probabili conseguenze della violazione;
- descrizione delle misure adottate o proposte per porre rimedio alla violazione ed eventualmente delle misure per mitigare i potenziali effetti negativi.

Per indicazioni su come identificare e segnalare una violazione dei dati, consultare il nostro **procedura e schema di notifica delle violazioni di dati personali**.

Cosa c'è da sapere

Che cos'è una **valutazione d'impatto sulla protezione dei dati?**

Una procedura di trattamento che venga utilizzata per la prima volta in azienda (ad esempio per un nuovo e-shop con un'opzione di pagamento, in modo che i dati personali dei clienti che acquistano online vengano elaborati da noi) deve essere innanzitutto verificata, per stabilire se serva allo scopo per cui è stata creata (ad esempio per il trattamento di indirizzi, nomi, informazioni bancarie per il pagamento online con carta di credito), se sia realmente necessaria e proporzionata al raggiungimento di detto scopo (ad esempio, ho bisogno di queste informazioni per effettuare un addebito sulla carta di credito? Potrei farlo anche con meno informazioni?), se esistano nuovi rischi potenziali per i dati personali (ad esempio, le informazioni bancarie potrebbero essere rubate con un attacco informatico esterno?) nonché come ridurre questi rischi potenziali e con quali misure (ad esempio, ho bisogno di un firewall più potente o di un altro antivirus per poter garantire la sicurezza delle informazioni bancarie?).

Che cos'è una **notifica della violazione di dati personali** o **Data Breach Notification?**

Qualsiasi violazione al nostro sistema di protezione (ad esempio, invio accidentale di un elenco di clienti con dati personali a un gruppo esterno più ampio di destinatari invece che a una persona specifica e autorizzata a riceverlo), deve essere notificata immediatamente al reparto Legal & Compliance all'indirizzo dataprotection@bmsuisse.ch. Si decide quindi se la violazione comporta un rischio elevato per le persone interessate (l'elenco riportava molti clienti? I dati erano particolarmente sensibili? I dati dell'elenco clienti sono ora potenzialmente utilizzati dai destinatari non autorizzati per l'invio di mailing o venduti ad altre aziende?).

Una segnalazione a dataprotection@bmsuisse.ch deve contenere almeno le seguenti informazioni:

- descrizione del tipo di violazione (ad esempio invio di un elenco clienti a x persone, si tratta dei dati di x clienti come nome, indirizzo ecc.);
- descrizione delle probabili conseguenze della violazione (i dati del cliente potrebbero ora essere utilizzati per un trattamento per il quale non erano originariamente destinati e per il quale non abbiamo il consenso);
- misure proposte (potremmo inviare una mail a tutti e informarli che devono cancellare/non utilizzare i dati di questi clienti).

12. Compliance/Reporting

All'individuazione di un difetto di conformità, il reparto Legal & Compliance, in collaborazione con l'azienda BMS interessata, definisce una procedura e tempistiche adeguate per soddisfare i requisiti entro un periodo di tempo ragionevole e specificato. I casi gravi vengono segnalati alla direzione, che ne assume la gestione.

13. Organizzazione

13.1 Direzione

La direzione definisce i principi generali necessari a garantire la protezione dei dati nelle aziende BMS. Nomina un centro di contatto competente, incaricato di far rispettare i requisiti in materia di protezione dei dati.

13.2 Superiori

I superiori a tutti i livelli rispondono dell'applicazione e del rispetto delle disposizioni in materia di protezione dei dati in conformità con la presente direttiva nelle loro aree di responsabilità. Essi provvedono alla formazione e alla sensibilizzazione del proprio personale in collaborazione con il centro di contatto. Consapevoli di dover essere di esempio, promuovono la motivazione dei collaboratori a rispettare le misure di protezione dei dati.

13.3 Centro di contatto competente

Il reparto Legal & Compliance è il centro di contatto competente nominato dalla direzione.

Il reparto Legal & Compliance ha la responsabilità di documentare la presente direttiva sulla protezione dei dati.

La Data Protection Task Force (composta da collaboratori dei reparti Legal & Compliance, IT e HR) affianca le aziende BMS nell'applicazione e nell'implementazione della protezione dei dati.

Il reparto Legal & Compliance monitora e tiene conto dell'evoluzione dei requisiti legali in materia di protezione dei dati.

13.4 Tutti gli altri collaboratori

Tutti i collaboratori delle aziende BMS devono leggere e rispettare la versione più recente della presente direttiva sulla protezione dei dati (disponibile su BMSmobile al link interno ASTRA).

I collaboratori che violino intenzionalmente la presente direttiva sulla protezione dei dati possono essere soggetti ad azioni disciplinari, fino al licenziamento.

13.5 Responsabili

13.5.1 Rapporti con l'esterno

Ciascuna azienda BMS è responsabile dei rapporti con l'esterno.

Il responsabile del trattamento mette in atto misure tecniche e organizzative adeguate, in particolare tenendo conto della natura, dell'ambito di applicazione, delle circostanze e delle finalità del trattamento e della diversa probabilità e gravità dei rischi per i diritti e le libertà delle persone fisiche, al fine di garantire ed essere in grado di dimostrare che il trattamento viene effettuato in conformità al RGPD e alla LPD.

13.5.2 Rapporti interni

Il responsabile del reparto HR e i suoi collaboratori rispondono dell'accuratezza del trattamento dei dati personali nel rispetto delle relative norme di protezione per la loro area di competenza a livello interno.

Il responsabile del reparto IT ha il compito di garantire internamente che le misure di sicurezza e protezione dei dati siano implementate in modo tecnicamente appropriato, in particolare con il supporto dei responsabili di applicazioni e sistemi. Egli opera a stretto contatto con il reparto Legal & Compliance per verificare la conformità delle misure, valutando i rischi, gli incidenti e i quasi incidenti che possono mettere a repentaglio la protezione dei dati.

Cosa c'è da sapere

La **direzione** definisce i principi per la protezione dei dati. I casi gravi di violazione della protezione dei dati devono essere segnalati alla direzione.

Tutti i **superiori** devono attenersi ai principi della protezione dei dati in modo esemplare. Essi devono garantire che i loro collaboratori siano informati sulla presente direttiva e sui principi della protezione dei dati, fornendo loro adeguati corsi di formazione, laddove necessario.

Il reparto **Legal & Compliance** è il centro di contatto per le domande, per la compilazione del registro, per l'aggiunta di nuove procedure di trattamento al registro, per la redazione di documenti sulla protezione dei dati, per le richieste di informazioni, accesso, rettifica, modifica e cancellazione, per le notifiche relative alle violazioni della protezione dei dati e per tutte le altre questioni riguardanti la protezione dei dati.

Tutti i collaboratori si impegnano a rispettare la presente direttiva sulla protezione dei dati di un'azienda BMS nel momento in cui instaurano un rapporto di lavoro con la stessa.

Esternamente, la responsabilità della protezione dei dati è a carico delle aziende BMS.

A livello **interno,** i principali responsabili sono i reparti Legal & Compliance, IT (per le misure tecniche, l'esecuzione di valutazioni d'impatto sulla protezione dei dati e la verifica delle notifiche di violazione) e HR (per i dati personali particolarmente sensibili e per i dati dei collaboratori in generale), ma la protezione dei dati personali è un dovere di tutti i collaboratori.

14. Disposizioni finali

14.1 Emendamenti e integrazioni

La presente direttiva sulla protezione dei dati può essere modificata, integrata o abrogata per iscritto dal reparto Legal & Compliance. Con emendamento o integrazione si intende qualsiasi aggiunta, eliminazione o modifica di singole disposizioni, con l'eccezione di correzioni di natura formale e di errori di trascrizione.

14.2 Documenti complementari

La presente direttiva costituisce il fondamento per le disposizioni in materia di protezione dei dati delle aziende BMS, da cui possono derivare istruzioni e altri documenti necessari per il trattamento dei dati personali.

14.3 Parti integranti

I seguenti allegati costituiscono parte integrante della presente direttiva sulla protezione dei dati:

1. Procedura in caso di richieste di informazioni, rettifica e cancellazione

2. Richiesta di cancellazione interna

3. Richiesta di cancellazione esterna

4. Richiesta di rettifica interna

5. Richiesta di rettifica esterna

6. Richiesta di cancellazione interna

7. Richiesta di cancellazione esterna

8. Concetto per la valutazione d'impatto sulla protezione dei dati

9. Procedura e schema Data Breach Notification

14.4 Varie

La presente direttiva sulla protezione dei dati è a disposizione di tutti i collaboratori tramite BMSmobile.

Il reparto Legal & Compliance ha la responsabilità di documentare la presente direttiva sulla protezione dei dati. Tutte le domande sull'argomento devono essere inviate a dataprotection@bmsuisse.ch.

Eventuali emendamenti o integrazioni di rilievo alla presente direttiva sulla protezione dei dati vengono comunicati ai collaboratori delle aziende BMS dal reparto HR ed entrano in vigore al momento della loro pubblicazione su BMSmobile.

14.5 Entrata in vigore

La presente direttiva sulla protezione dei dati entra in vigore settembre 2022.