

Esecuzione di una valutazione d'impatto sulla protezione dei dati

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

Piano sintetico

BMS Building Materials Suisse (**BMS**) prende molto sul serio la protezione dei dati personali e il rispetto delle leggi in materia, assoggettandosi pertanto al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, noto come Regolamento generale sulla protezione dei dati (RGPD) e alla Legge svizzera sulla protezione dei dati (LPD), in quanto la società madre BME ha sede nei Paesi Bassi mentre BMS ha sede e opera in Svizzera. Questo comporta dei doveri per BMS, tra cui l'obbligo di eseguire valutazioni d'impatto sulla protezione dei dati per le attività di trattamento dei dati personali di nuova pianificazione che possono comportare un rischio elevato per i diritti e le libertà delle persone fisiche, come previsto dall'art. 35 del RGPD e dall'art. 20 f della LPD, spettante a BMS in quanto parte responsabile. BMS affida l'effettiva esecuzione delle valutazioni d'impatto sulla protezione dei dati e tutti i relativi poteri ai reparti Legal & Compliance e IT, tuttavia consapevole della propria immutata responsabilità.

La valutazione d'impatto sulla protezione dei dati è una procedura volta a descrivere il trattamento in esame, a vagliarne la necessità e la proporzionalità e a consentire un migliore controllo dei rischi per i diritti e le libertà delle persone fisiche posti dal trattamento dei dati personali attraverso una loro adeguata analisi e l'individuazione di misure di attenuazione. Una valutazione d'impatto sulla protezione dei dati è quindi una procedura con cui garantire e dimostrare la conformità ai requisiti di legge.

Questo piano sintetico illustra le fasi necessarie alla creazione di una procedura di test e verifica affidabile nel lungo termine:

Fase 1: registro delle attività di trattamento

Il registro delle attività di trattamento esistenti di BMS può essere visualizzato e modificato solo dal reparto Legal & Compliance ed è protetto di conseguenza mediante misure tecniche e organizzative adeguate.

L'assenza all'interno di BMS di attività di trattamento specifiche richieste al momento dell'introduzione di nuovi prodotti o progetti o dell'utilizzo di nuove tecnologie deve essere segnalata dal responsabile del prodotto, del progetto o della nuova tecnologia (**persona responsabile**) per e-mail a dataprotection@bmsuisse.ch.

Fase 2: preparazione di una valutazione dei rischi per le nuove attività di trattamento notificate

Se il reparto Legal & Compliance, dopo un primo breve esame della nuova attività di trattamento notificata utilizzando la lista di controllo «Valutazione dei rischi delle attività di trattamento» (non pubblica), decide che è necessario effettuare una valutazione d'impatto sulla protezione dei dati, convoca a tal fine la Data Protection Task Force (**DP Task Force**). La DP

Task Force è composta da membri selezionati dei reparti Legal & Compliance, IT, HR e dalla persona responsabile.

Le liste di controllo compilate servono come prova della verifica della necessità di una valutazione d'impatto sulla protezione dei dati e devono essere conservate in modo sicuro dal reparto Legal & Compliance, indipendentemente dal risultato.

Fase 3: dove necessario, esecuzione di una valutazione d'impatto sulla protezione dei dati

Qualora il reparto Legal & Compliance stabilisca invece la necessità di una valutazione d'impatto sulla protezione dei dati, documenta la propria decisione con la lista di controllo di cui sopra, informa la persona responsabile che l'esecuzione dell'attività di trattamento verificata (la nuova procedura/app, del nuovo servizio/sistema ecc.) è sospesa fino a nuovo avviso e convoca la DP Task Force per avviare la valutazione d'impatto sulla protezione dei dati.

La persona responsabile deve sospendere la rispettiva attività di trattamento (della nuova procedura/app, del nuovo servizio/sistema ecc.) fino all'esito della valutazione d'impatto sulla protezione dei dati.

Il reparto Legal & Compliance avvia quindi la procedura per la valutazione d'impatto sulla protezione dei dati con la DP Task Force in conformità con le linee guida previste per l'esecuzione di detta attività (non pubbliche).

La DP Task Force dispone ora di un periodo di quattordici (14) giorni lavorativi (un'estensione del termine è a discrezione del reparto Legal & Compliance, ma deve poter essere giustificata) per condurre la valutazione d'impatto sulla protezione dei dati e discutere le azioni correttive appropriate.

Fase 4: verifiche regolari

La DP Task Force ha il compito di verificare le valutazioni d'impatto sulla protezione dei dati

A) **ogni (3) anni**

o

B) **in qualsiasi momento, laddove** si verifichino **cambiamenti** dei rischi legati alle procedure di trattamento