# Regolamento del processo di gestione e segnalazione delle violazioni dei dati personali (data breach)

Procedura emessa il: 31/08/2021
Aggiornata il: 24/11/2022
Owner della procedura: Perspective Augmented Intelligence

**Indice**

# 1 Premessa

Il regolamento europeo n. 679/2016 sulla protezione dei dati personali (*General Data Protection Regulation*, di seguito anche - GDPR) include tra i suoi obiettivi l'adozione di misure tecniche e organizzative di trattamento dei dati personali, tali da garantire un'adeguata sicurezza dei dati personali, compresa la protezione da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

A tal fine, il regolamento richiede che sia i Titolari che i Responsabili del trattamento dei dati personali definiscano processi e procedure efficaci in grado di rilevare e limitare tempestivamente gli effetti di una violazione, valutare il rischio per i soggetti impattati e stabilire se sia necessario notificare la violazione al Garante per la Protezione dei dati personali (di seguito anche Garante) e comunicarla alle persone interessate, ove necessario. In caso di incidente, la notifica al Garante costituisce una parte del piano di intervento.

L'obiettivo di tale comunicazione è quello di consentire al Garante di attivarsi tempestivamente, valutare la gravità della situazione e stabilire le misure correttive da imporre al Titolare per ridurre al minimo i pericoli per la *privacy* degli interessati a cui si riferiscono i dati.

In particolare, il regolamento impone al Titolare dei dati personali di notificare la violazione senza ingiustificato ritardo e, ove possibile, entro 72 (settantadue) ore "dal momento in cui è stata accertata la violazione".

La violazione viene descritta secondo il modello di comunicazione messo a disposizione dal Garante attraverso i canali preposti.

## 1.1 AMBITO DI APPLICAZIONE

Il processo descritto dal presente Regolamento si applica a Flowe Società Benefit (di seguito anche Flowe o la Società).

## 1.2 PERIMETRO DI RIFERIMENTO

Il processo in oggetto si applica a tutti gli eventi che comportano una violazione di dati personali successivamente alla data di prima pubblicazione del presente Regolamento.

Con il termine "violazione dei dati personali" (di seguito anche *data breach*) si intende un qualunque evento che comporti, anche accidentalmente o in modo illecito (e per un periodo di tempo limitato), la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Con riferimento al modello operativo del Conglomerato Finanziario Mediolanum, i *data breach* possono interessare dati personali contenuti su documentazione:

- "cartacea", conservata presso la Sede di Milano3 della Società, le sedi dei fornitori della Società e delle altre società che con Flowe collaborano; rientrano nel perimetro anche i *data breach* relativi a documenti in transito dalle sedi delle società che collaborano con Flowe verso la sede della Società o viceversa;
- "elettronica", presenti su dispositivi e/o archivi elettronici quali ad esempio *database*, *personal computer*, dispositivi cellulari, chiavette USB, altre unità di archiviazione esterna) in uso al personale dipendente o a collaboratori esterni di Flowe e delle società che con Flowe collaborano nonché tutti i soggetti autorizzati al trattamento.

Tale perimetro comprende inoltre violazioni dei dati personali gestiti da risorse e/o sistemi informativi di fornitori in qualità di Responsabili del trattamento dei dati o di soggetti autorizzati al trattamento; tali soggetti segnalano a Flowe, "senza ingiustificato ritardo", la violazione. In questo caso, il Responsabile non effettua alcuna valutazione in merito alla probabilità di rischio derivante dal *data breach*, ma fornisce a Flowe tutti i

dati e le informazioni per determinare la rischiosità dell'evento e decidere in merito alla segnalazione al Garante per la protezione dei dati personali.

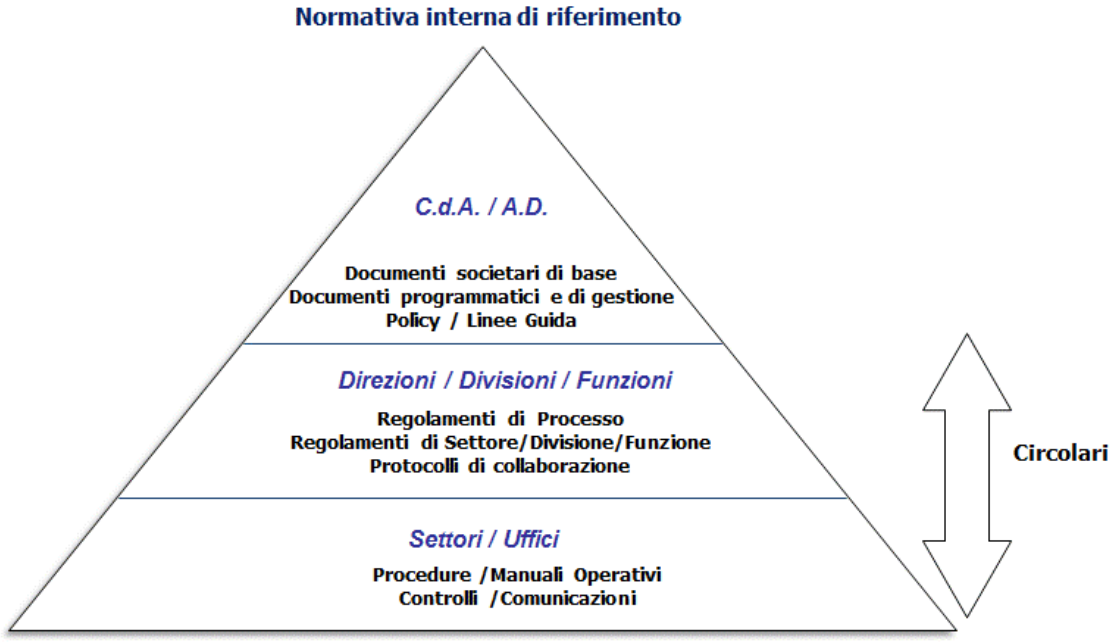
Non rientrano invece nell'ambito di applicazione del presente regolamento, i possibili «*data breach*» rilevati da soggetti che sono Titolari del trattamento dei dati personali; tali violazioni sono rilevate, valutate ed eventualmente segnalate al Garante dallo stesso soggetto Titolare.

## 1.3 OBIETTIVI DEL DOCUMENTO

Il presente documento ha l'obiettivo di:

- descrivere le diverse fasi del processo di gestione e segnalazione delle violazioni dei dati personali;
- richiamare ruoli e responsabilità degli attori coinvolti nel processo.

Con riferimento alla "*Policy di Gruppo sulle modalità di redazione, approvazione, diffusione ed aggiornamento della Normativa interna*", il presente documento si colloca al secondo livello della piramide documentale richiamata nello schema seguente.




## 1.4 STRUTTURA DEL DOCUMENTO

Il Regolamento si compone complessivamente di 4 capitoli oltre al presente. Di seguito sono descritte sinteticamente le principali tematiche trattate in ogni capitolo:

**Capitolo 2: Gli attori coinvolti**

Obiettivo del Capitolo è descrivere e richiamare in modo chiaro ruolo e responsabilità degli attori coinvolti nel processo oggetto del presente documento, definendo modalità di interazione e coordinamento previste nei casi di processo di carattere interfunzionale.

**Capitolo 3: Il processo**

Obiettivo del Capitolo è descrivere gli aspetti di carattere organizzativo, il processo e le modalità di interazione con altre entità organizzative o società terze, interne o esterne alla Società od al Gruppo Mediolanum, in relazione al processo oggetto di

regolamentazione, gli strumenti utilizzati e gli output attesi dalle fasi in cui il processo è articolato.

**Capitolo 4: Il contesto normativo esterno**

Obiettivo del Capitolo è descrivere il quadro normativo esterno di riferimento nell'ambito rilevante per il processo oggetto di regolamentazione (es. normativa di primo e secondo livello).

**Capitolo 5: Le policy e la normativa interna di riferimento**

Obiettivo del Capitolo è descrivere le fonti normative interne al Gruppo Mediolanum (es. *policy*, procedure operative, regolamenti di processo) che presentano relazioni con il processo in esame.

# 2 Gli attori coinvolti

Il modello organizzativo adottato dalla Società prevede il coinvolgimento delle *perspective* della Società, di opportune funzioni della Capogruppo Banca Mediolanum (che svolgono in *outsourcing* servizi aziendali in virtù di un apposito accordo di esternalizzazione) e delle strutture organizzative degli *outsourcer* tecnologici, che si impegnano, per quanto di competenza, ad applicare il presente regolamento.

Gli attori, ovvero le unità organizzative coinvolte a vario titolo nel processo di gestione e segnalazione delle violazioni di dati personali sono di seguito richiamati, con evidenza esclusivamente del ruolo specificatamente attribuito nel processo medesimo.

## 2.1 Consiglio di Amministrazione

Il *Consiglio di Amministrazione di Flowe* (di seguito anche *CdA*) è il Titolare del trattamento, cioè il soggetto cui competono, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo di sicurezza. È il reale ed effettivo soggetto che esercita in completa autonomia il potere decisionale sull'attività di gestione dei dati.

I componenti del *Consiglio di Amministrazione di Flowe* sono informati dei *data breach* più critici per la Società.

## 2.2 Amministratore Delegato

L'*Amministratore Delegato di Flowe*, in qualità di Legale Rappresentante della Società, viene coinvolto dal *DPO* di Flowe nei casi di *data breach* più critici per la Società; decide, con il supporto del *Delegato del Titolare del Trattamento* in merito alla segnalazione al Garante e se necessario agli interessati, dei *data breach* critici per la Società.

In tutti i casi di *data breach*, valuta se effettuare un'informativa al *CdA* e se segnalare alle opportune strutture della Capogruppo le caratteristiche rilevanti dell'evento.

## 2.3 Delegato del Titolare del Trattamento

Nel modello organizzativo sul trattamento dei dati del Conglomerato Finanziario Mediolanum, al fine di una migliore gestione degli adempimenti strettamente connessi alla normativa di riferimento, Flowe ha nominato un soggetto qualificato cui delegare gli adempimenti propri del Titolare.

Il *Delegato del Titolare del Trattamento* (di seguito anche *Delegato Privacy*) è nominato e risponde direttamente al Consiglio di Amministrazione.

Nell'ambito del processo in oggetto il *Delegato Privacy* di Flowe è informato dal *Data Protection Officer* (di seguito *DPO*) o dall'*Ufficio Privacy di Banca Mediolanum* di tutte le attività e fasi di gestione del *data breach*. A fronte delle valutazioni e degli esiti della discussione con i componenti del *Data Breach Team*, riceve una relazione contenente le

evidenze del *data breach*, i rischi rilevati, le azioni di risoluzione e/o di mitigazione identificate e la necessità o meno di segnalare l'evento al Garante.

In caso di *data breach* critici e rilevanti valuta le modalità e le tempistiche di coinvolgimento dell'*Amministratore Delegato* con il relativo giudizio sulla criticità e rilevanza dell'evento.

In qualità di *Delegato del Titolare del Trattamento* può decidere in merito alla segnalazione dell'avvenuta violazione all'Autorità e se necessario agli interessati; in caso di necessità di notificare l'evento, verifica i contenuti del rapporto di segnalazione ed esegue le attività di inoltro al Garante.

Qualora sia necessario comunicare il *data breach* agli interessati, prende visione anche dei contenuti della comunicazione prima dell'invio della stessa.

### 2.4 UFFICIO PRIVACY DI BANCA MEDIOLANUM

In forza del contratto di appalto di fornitura dei servizi di gestione aziendale in essere tra Banca Mediolanum e Flowe, l'*Ufficio Privacy di Banca Mediolanum*, nell'ambito del processo oggetto del presente regolamento:

- presidia la casella di posta elettronica dedicata alla raccolta delle segnalazioni relative a possibili violazioni di dati personali (segnalazionigdpr@mediolanum.it);
- prende in carico le segnalazioni ed effettua le valutazioni preventive propedeutiche all'identificazione (o meno) del *data breach*;
- se necessario, richiede al soggetto segnalatore eventuali informazioni aggiuntive in merito all'incidente oppure coinvolge le unità organizzative aziendali nella raccolta di dati ed elementi necessari all'identificazione del *data breach*;
- supporta il *DPO* nella fase di valutazione dei rischi per le libertà e diritti degli interessati determinati dal *data breach*;
- in caso di segnalazione al Garante, predispone i contenuti del rapporto di comunicazione e li sottopone alla verifica da parte del *DPO* e del *Delegato Privacy*;
- in caso di segnalazione agli interessati predispone, in collaborazione con la *Perspective Business Acceleration* e il *DPO*, i contenuti della comunicazione, coinvolgendo se necessario le unità organizzative interessate;
- censisce tutte le segnalazioni di violazione di dati personali ricevute (comprese quelle non corrispondenti a *data breach*) all'interno del Registro delle violazioni;
- supporta il *DPO* nel controllo dello stato di esecuzione del piano di intervento comunicato al Garante.

L'Ufficio è inoltre responsabile del presidio del modello e della normativa di riferimento in tema di *data breach*.

### 2.5 DATA PROTECTION OFFICER

Il *Data Protection Officer di Flowe* viene tempestivamente informato dall'*Ufficio Privacy di Banca Mediolanum* della rilevazione di una violazione dei dati personali ed è coinvolto durante tutto il processo di gestione ed eventuale segnalazione al Garante.

In particolare:

- nella fase di verifica preliminare, esprime un parere su tutte le valutazioni effettuate dal *Delegato Privacy* o dall'*Ufficio Privacy di Banca Mediolanum*, comprese quelle "negative" (non corrispondenti a *data breach*);
- verifica, con il supporto del *Delegato Privacy*, se «il *data breach* possa determinare rischi per le libertà e diritti degli interessati»;
- valuta, di volta in volta, la necessità di attivare il *Data Breach Team* per la definizione del piano di intervento complessivo da comunicare al Garante;

- a fronte delle valutazioni e della disamina con i componenti del *Data Breach Team*, redige una relazione in cui raccoglie le evidenze del *data breach*, i rischi, le azioni di risoluzione e/o mitigazione identificate e la necessità o meno di segnalare l'evento al Garante;
- condivide i contenuti della «relazione» con il *Delegato Privacy*;
- verifica i contenuti del rapporto e della comunicazione agli interessati (ove richiesto);
- effettua, in caso di assenza o impedimento del *Delegato Privacy*, l'invio del rapporto di segnalazione della violazione al Garante;
- predispone un'informativa relativa alle segnalazioni di *data breach*, contenute nel registro delle violazioni, nell'ambito della relazione periodica da sottoporre all'attenzione del *CdA*.

Nella fase di monitoraggio del piano di intervento, verifica che le azioni definite siano gestite secondo le modalità e le tempistiche comunicate al Garante, notificando al Garante eventuali differenze o ritardi rispetto a quanto notificato.

## 2.6 DATA BREACH TEAM

Il *Data Breach Team* svolge una funzione di supporto al *Data Protection Officer* in caso di violazioni di dati personali con potenziali rischi per i diritti e le libertà degli interessati.

In particolare:

- supporta il *DPO* e il *Delegato Privacy* nelle valutazioni sui rischi per i diritti e le libertà degli interessati (potenziali ed effettivi) determinati del *data breach*;
- identifica (ed avvia) le azioni per contenerne e/o minimizzarne i rischi nonché evitare che si verifichino nuovamente eventi similari.

Il *Data Breach Team* viene convocato all'occorrenza a discrezione del *DPO*, in base alla natura e all'entità dell'incidente e comunque in tempo utile per svolgere i propri compiti.

Il *Data Breach Team* di Flowe è composto da:

- *Data Protection Officer*, con ruolo di coordinatore;
- *Delegato Privacy*
- Responsabile della *Perspective Augmented Intelligence*
- Responsabile della *Perspective Happiness and Service*;
- Responsabile della *Perspective Business Acceleration;*
- Responsabile della *Funzione Risk Management*;
- Responsabile della *Funzione Compliance*;
- Responsabile della *Divisione Affari Legali di Banca Mediolanum*.

## 2.7 PERSPECTIVE AUGMENTED INTELLIGENCE

La *Perspective Augmented Intelligence* supporta l'*Ufficio Privacy di Banca Mediolanum* e il *DPO* nelle fasi di verifica preliminari e comunica agli stessi e alle Perspective interessate lo stato di avanzamento delle azioni tecniche risolutive e/o di mitigazione di un *data breach* collegato ad un incidente di sicurezza informatica.

## 2.8 PERSPECTIVE HAPPINESS AND SERVICE

La *Perspective Happiness and Service*:

- riceve la segnalazione di una violazione della sicurezza di dati relativi alla clientela;
- partecipa all'attività di verifica utile alla definizione di un possibile evento di *data breach* o di risoluzione di un evento già identificato;

- supporta l'*Ufficio Privacy di Banca Mediolanum* nelle fasi di verifica preliminari, raccogliendo e fornendo i dati e le informazioni necessarie alla classificazione dell'incidente e al monitoraggio delle attività di risoluzione dello stesso;
- partecipa alla predisposizione dell'eventuale comunicazione agli interessati ed è responsabile dell'invio della stessa individuandone la modalità in base al tipo di evento, all'urgenza, ai volumi dei soggetti interessati;
- comunica al *DPO* e alle unità organizzative interessate lo stato di avanzamento (compresi eventuali aspetti di criticità) delle azioni tecniche risolutive e/o di mitigazione di un *data breach*.

### 2.9 PERSPECTIVE BUSINESS ACCELERATION

Qualora i soggetti interessati dal *data breach* siano clienti, la *Perspective Business Acceleration* collabora con l'*Ufficio Privacy di Banca Mediolanum* nella predisposizione dei contenuti delle comunicazioni da inoltrare ai clienti.

### 2.10 SETTORE CONTENZIOSO

In forza del contratto di appalto di fornitura dei servizi di gestione aziendale in essere tra Banca Mediolanum e Flowe, il *Settore Contenzioso e Reclami di Banca Mediolanum* supporta il *Delegato Privacy*, il *DPO* e l'*Ufficio Privacy di Banca Mediolanum* su potenziali conseguenze in termini di contenzioso.

### 2.11 FUNZIONE RISK MANAGEMENT

La *Funzione Risk Management* di Flowe viene coinvolta dal *DPO* e dall'Ufficio Privacy al fine di effettuare con il supporto della *Perspective Business Acceleration* una prima valutazione dell'impatto reputazionale derivante dal *data breach*, ossia il livello di visibilità che l'incidente ha ricevuto o riceverà sul mercato e la probabilità che causi danni alla reputazione della Società o delle altre società del Conglomerato Finanziario Mediolanum.

### 2.12 UNITÀ BUSINESS CONTINUITY OFFICE & DIGITAL PROCESS AUTOMATION DI BANCA MEDIOLANUM

In forza del contratto di appalto di fornitura dei servizi di gestione aziendale in essere tra Banca Mediolanum e Flowe, l'*Unità Business Continuity Office & Digital Process Automation di Banca Mediolanum* viene attivata in caso di violazioni di dati personali derivanti da incidenti di sicurezza informatica che generano indisponibilità dei sistemi informativi; e in questo caso valuta le tempistiche e le modalità di attivazione del *Comitato di Crisi e Business Continuity*.

### 2.13 SETTORE CONSULENZA E CONTRATTUALISTICA DI BANCA MEDIOLANUM

In forza del contratto di appalto di fornitura dei servizi di gestione aziendale in essere tra Banca Mediolanum e Flowe, il *Settore Consulenza e Contrattualistica di Banca Mediolanum* fornisce supporto al *DPO* e all'Ufficio Privacy nel valutare l'inquadramento e la formalizzazione degli atti e dei rapporti che hanno determinato il *data breach*.

Il Settore verifica inoltre i testi delle comunicazioni da inoltrare ai soggetti che hanno subito una violazione dei dati personali.

### 2.14 DIREZIONE RISORSE UMANE DI BANCA MEDIOLANUM

In forza del contratto di appalto di fornitura dei servizi di gestione aziendale in essere tra Banca Mediolanum e Flowe, qualora i soggetti interessati dal *data breach* siano dipendenti della Società, la *Direzione Risorse Umane di Banca Mediolanum* collabora con l'*Ufficio Privacy di Banca Mediolanum* nella definizione del piano di intervento e nella predisposizione dei contenuti della comunicazione da inoltrare.

## 2.15 ATTORI ESTERNI

### 2.15.1 CLIENTI

Nell'ambito di un *data breach*, i clienti possono assumere un ruolo:

- attivo: segnalando possibili eventi di violazione della sicurezza dei dati personali (es.: ricezione di documentazione ufficiale ma inerenti ad altri clienti);
- passivo: in quanto il verificarsi di un *data breach* presuppone un danno/pericolo alla propria *privacy* e ne devono essere informati.

### 2.15.2 FORNITORI DI SERVIZI

I fornitori identificati come Responsabili del trattamento dei dati sono tenuti a segnalare alla Società "senza ingiustificato ritardo", la violazione, fornendo tutti i dati e le informazioni necessarie a determinare la rischiosità dell'evento e decidere in merito alla segnalazione al Garante per la protezione dei dati personali.

I fornitori identificati come Titolari del trattamento dei dati personali valutano ed eventualmente segnalano al Garante i *data breach* rilevati, dandone opportunamente evidenza a Flowe al fine di concordare le modalità di comunicazione nei confronti dei soggetti collegati.

### 2.15.3 ALTRI SOGGETTI ESTERNI A FLOWE

I potenziali clienti o altri soggetti che non hanno alcun rapporto con Flowe (es.: autorità giudiziaria), possono rilevare eventi di *data breach* che interessano la Società ed eventualmente segnalarli secondo i canali messi a disposizione dalla Società stessa.

# 3 Il processo

Il presente Regolamento illustra i principi guida, l'architettura organizzativa e le interdipendenze alla base del processo di gestione e segnalazione delle violazioni dei dati personali.

Di seguito è rappresentato il processo nella sua articolazione complessiva:


## 3.1 RILEVAZIONE ED INOLTRO SEGNALAZIONE

Incidenti di sicurezza che possono comportare violazioni di dati personali possono essere rilevati da:

- Qualunque dipendente della Società;
- Clienti della Società;
- Fornitori;
- Altri soggetti, es.: clienti *prospect*, e altri soggetti senza alcun rapporto con la Società (es.: Autorità giudiziarie).

Le possibili segnalazioni di violazione alla sicurezza dei dati personali sono comunicate all'*Ufficio Privacy di Banca Mediolanum* attraverso l'invio di una e-mail alla casella di posta elettronica dedicata (segnalazionigdpr@mediolanum.it).

Il soggetto segnalatore, oltre a descrivere l'evento e a comunicare il tipo di dati interessati e di soggetti potenzialmente coinvolti, se possibile, compila ed inoltra il modulo di «raccolta della segnalazione», così da indirizzare correttamente le attività di identificazione del *data breach* e di verifiche preliminari.

Il soggetto segnalatore dell'incidente fornisce all'*Ufficio Privacy di Banca Mediolanum*:

- i dati identificativi (comprensivi di indirizzo mail e numero di telefono) di chi ha rilevato il potenziale *data breach*;
- una breve descrizione dell'evento comunicando ora, data, luogo e le possibili cause (se individuate);
- la tipologia dei soggetti interessati (minori o soggetti vulnerabili, dipendenti, collaboratori/famigliari, clienti/*prospect*, potenziali terze parti, fornitori, ed altri);
- la tipologia dei dati potenzialmente interessati (identificativi, comportamentali, bancari, sensibili, giudiziari, di geolocalizzazione, gestione del rapporto di lavoro, *cookies*, utenze di sistema, ed altro);
- stima e dimensione dei *record* coinvolti.

## 3.2 VERIFICHE PRELIMINARI

In questa fase, sulla base dei dati contenuti nel modulo di «segnalazione» e delle ulteriori informazioni raccolte, viene verificato dal *DPO* che la segnalazione corrisponda o meno ad un *data breach*. Nel caso in cui il *data breach* segnalato:

- non sia riconosciuto come tale, la segnalazione viene chiusa e archiviata nel «registro delle violazioni»;
- sia riconosciuto come possibile, si procede con le attività di analisi e valutazione dei relativi rischi.

I termini per l'eventuale segnalazione al Garante decorrono "dal momento in cui il Titolare ha accertato la violazione".

Tutte le segnalazioni, comprensive delle valutazioni preventive dell'*Ufficio Privacy di Banca Mediolanum* e dei dati raccolti sono sottoposte all'attenzione del *DPO* della/e Società interessata/e, che esprime un parere.

A tal proposito, l'*Ufficio Privacy di Banca Mediolanum* e il *DPO*, in base alla natura del *data breach* coinvolgono le unità organizzative che possano fornire supporto alla raccolta di dati ed elementi necessari all'identificazione del *data breach*.

Tutte le segnalazioni corrispondenti a possibili *data breach* e che saranno oggetto di analisi e di valutazioni più approfondite sono notificate al *Delegato del Titolare del Trattamento* dei dati.

## 3.3 VALUTAZIONE DEI RISCHI E DEFINIZIONE DEL PIANO DI INTERVENTO

In questa fase, coerentemente con quanto previsto dalle Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679 l'*Ufficio Privacy di Banca Mediolanum*, con il supporto del *DPO*, valuta se "il *data breach* possa determinare rischi per le libertà e diritti degli interessati".

Nella valutazione del rischio sono coinvolti, se necessario, anche la *Funzione Risk Management* e la *Perspective Augmented Intelligence* (in caso di incidenti di sicurezza informatica o incidenti applicativi), che possano fornire supporto alla raccolta di dati ed elementi necessari alla valutazione.

Se non si rilevano rischi per le libertà e diritti degli interessati, la segnalazione viene chiusa e archiviata nel registro delle violazioni della Società e non è necessario effettuare alcuna comunicazione del *data breach* né al Garante né agli interessati; l'*Ufficio Privacy di Banca Mediolanum* procede in ogni caso ad informare il *Delegato Privacy*. A seconda della natura del *data breach* e dei relativi dati impattati, possono essere comunque identificate (e avviate) delle azioni di risoluzione o di mitigazione.

In caso di valutazione di "rischi non alti", è comunque necessario procedere con la segnalazione del *data breach* al Garante, mentre qualora vengano identificati dei rischi alti, si procede sia con la segnalazione al Garante che ai soggetti interessati.

In base alla natura del *data breach* e alla eventuale necessità di predisporre un piano di interventi, il *DPO* valuta, di volta in volta, la necessità di attivare il *Data Breach Team*, che esprime un parere delle valutazioni sui rischi determinati dal *data breach* ed identifica (ed avvia se possibile) le azioni per contenerne e/o minimizzarne i rischi (nonché evitare che si verifichi nuovamente).

In caso di *data breach* e contestuale indisponibilità di sistemi informativi, il *DPO* attiva, la *Perspective Augmented Intelligence* che valuta se coinvolgere l'*Unità Business Continuity Office & Digital Process Automation di Banca Mediolanum* che valuta le tempistiche e le modalità di attivazione del *Comitato di Crisi e Business Continuity*.

A fronte delle valutazioni e degli esiti della discussione con i componenti del *Data Breach Team*, il *DPO* redige una relazione in cui raccoglie le evidenze del *data breach*, i rischi, le azioni identificate e la necessità o meno di notificare al Garante e la condivide con il *Delegato Privacy*. Nelle casistiche di *data breach* più critici e rilevanti viene, inoltre, informato l'*Amministratore Delegato* che valuterà la necessità di informativa al *CdA*.

## 3.4 INOLTRO COMUNICAZIONI AGLI STAKEHOLDERS

Quando la violazione dei dati personali presenta un rischio elevato per i diritti e le libertà delle persone fisiche, è necessario comunicare la violazione, senza ingiustificato ritardo:

- al Garante per la protezione dei dati personali;
- ai soggetti interessati.

### 3.4.1 COMUNICAZIONE AL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Come anticipato, la segnalazione al Garante deve essere effettuata nelle casistiche di *data breach* con rischi "non alti "ed "alti" per gli interessati entro 72 ore dall'accertamento del *data breach*.

Il rapporto di segnalazione viene compilato dall'*Ufficio Privacy di Banca Mediolanum* e verificato ed eventualmente integrato dal *DPO* e dal *Delegato Privacy*.

L'Amministratore Delegato prende visione del rapporto e valuta se effettuare un'informativa al *CdA*.

Qualora non siano disponibili tutte le informazioni richieste è prevista la possibilità di "notificare a fasi", eventuali ritardi nella segnalazione del *data breach*, devono essere opportunamente motivati.

Si specifica infine che in caso di *data breach* determinato da un grave incidente di sicurezza informatica, viene attivato il processo di segnalazione verso Banca d'Italia, secondo le tempistiche e le modalità previste dal Provvedimento di Banca d'Italia del 23 luglio 2019.

### 3.4.2 COMUNICAZIONE AI SOGGETTI INTERESSATI

In caso di alto rischio per gli interessati viene predisposta ed inviata anche una comunicazione agli stessi che contiene la natura del *data breach*, il contatto del *DPO*, le

misure implementate o pianificate per fronteggiare l'evento e i consigli per limitare le conseguenze dell'incidente.

La modalità di invio della comunicazione viene definita di volta in volta dalla *Perspective Happiness & Service* in base al tipo di evento, all'urgenza, ai volumi dei soggetti interessati e può essere costituita da una lettera cartacea, una email o un outbound.

La predisposizione delle comunicazioni è coordinata dall'*Ufficio Privacy di Banca Mediolanum* prevede il coinvolgimento delle seguenti unità organizzative:

- *Perspective Business Acceleration*, che in collaborazione con l'*Ufficio Privacy di Banca Mediolanum* definisce i contenuti della comunicazione, coinvolgendo se necessario eventuali altre *perspective* interessate;
- *DPO*, Divisione Affari Legali e *Delegato Privacy*, verificano i contenuti della comunicazione;
- *Amministrazione Delegato* che valida e sottoscrive la comunicazione;

### 3.5 *PERSPECTIVE HAPPINESS AND SERVICE* E *PERSPECTIVE AUGMENTED INTELLIGENCE* A SUPPORTO PER LA RACCOLTA DELLE INFORMAZIONI.MONITORAGGIO AZIONI

Le azioni risolutive e di mitigazione sono oggetto di monitoraggio periodico e di controlli sullo stato di esecuzione/completamento da parte del *DPO* della/e Società interessata/e.

Il *DPO*, eventualmente con il supporto dell'*Ufficio Privacy di Banca Mediolanum* accerta quindi che le azioni definite siano gestite secondo le modalità e le tempistiche comunicate al Garante e notifica al Garante eventuali differenze o ritardi rispetto a quanto notificato.

### 3.6 PRESIDIO DEL MODELLO

L'*Ufficio Privacy di Banca Mediolanum* presidia il modello di gestione e segnalazione delle violazioni dei dati personali sia in termini di verifica e controllo dello stato di evoluzione della normativa di riferimento, che di aggiornamento/affinamento dei criteri di valutazione di gravità di un *data breach*.
L'*Ufficio Privacy di Banca Mediolanum* è responsabile della segnalazione alle unità organizzative coinvolte nel processo, delle eventuali modifiche al processo e della necessità di rivedere le relative procedure operative di competenza.

## 4 La normativa esterna di riferimento

Nel presente capitolo si richiama il contesto normativo nel quale opera il presente Regolamento di processo.

Si riportano di seguito i principali riferimenti normativi:

- *Decreto Legislativo 10 agosto 2018 nr.101 e successivi aggiornamenti;*
- *Regolamento Europeo UE 2016/679 e successivi aggiornamenti;*
- *Provvedimento di Banca d'Italia del 23 luglio 2019 e successivi aggiornamenti.*

## 5 Le policy e la normativa interna di riferimento

Si riepilogano le fonti informative interne alla Banca che presentano relazioni con il processo in esame:

- *Privacy Policy di Banca Mediolanum;*
- *Policy per la gestione del rischio di reputazione;*
- *Policy di "Incident Management".*