Ettore **BATTELLI** Guido **D'IPPOLITO**

Compendio della PRIVACY, della CYBERSICUREZZA e dell'INTELLIGENZA ARTIFICIALE

III EDIZIONE 2026

Neldiritto Editore

categorie di soggetti che possono accedere a certe informazioni, riducendo così il perimetro di rischio di tali attività.

2. Violazione dei dati personali (*data breach*)

Dal principio di integrità e riservatezza di cui all'art. 5, par. 1, lett. g) del Regolamento, letto in combinato disposto con l'art. 32 RGPD, si ricava il concetto di **violazione dei dati personali**.
Per violazione dei dati personali si intende una **violazione della sicurezza** che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione o l'accesso non autorizzato ai dati personali (art. 4, n. 12, RGPD).
Tale nozione fa riferimento alla tripartizione delle violazioni propria dei principi di sicurezza informatica: **violazione dell'integrità dei dati**, che si verifica quando il titolare del trattamento non è più in grado di definire la qualità o verificare l'esattezza dei dati in suo possesso. Ciò avviene quando i dati sono stati alterati, manomessi o comunque in altro modo modificati al di fuori di alcuna autorizzazione o controllo del titolare; **violazione della riservatezza dei dati**, che si verifica quando i dati che dovrebbero essere conosciuti solo dal titolare, dall'interessato o dagli altri soggetti legittimamente preposti al trattamento, vengono resi pubblici o comunque accessibili a soggetti non autorizzati (è il caso, per esempio, della c.d. "esfiltrazione" dei dati); **violazione della disponibilità dei dati**, che si verifica quando il titolare del trattamento perde la disponibilità del dato che non sarà, quindi, più in suo possesso o sotto il suo controllo, oppure l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni (es. *malware* e *ransomware*).
A seconda delle circostanze, una violazione può essere integrata da una sola delle precedenti ipotesi o anche riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse.
Dunque, la violazione dei dati personali, comunemente conosciuta come "***data breach***", può dipendere da vari fattori: da errori tecnici e organizzativi del titolare o responsabile del trattamento o fattispecie illecite, come l'accesso abusivo ai sistemi informativi, fino a danni dovuti a comportamenti colposi o accidentali, come il furto o la perdita di dispositivi informatici contenenti dati personali (penna *usb*, *hard disk*, ecc.).
In base all'art. 32, par. 1, lett. b) del Regolamento, alla capacità di assicurare la riservatezza, l'integrità e la disponibilità dei dati si associa quella di garantire la **resilienza** dei sistemi e dei servizi di trattamento. Ossia, una volta concretizzatosi il rischio, è opportuno che il titolare abbia pensato e predisposto sistemi o procedure che permettano di ripristinare il trattamento nel più breve tempo possibile e riattivare il servizio in modo corretto, limitando quindi i danni già verificatisi.

3. Notifica all'autorità di controllo

In presenza di una violazione dei dati personali, o *data breach*, il Regolamento prevede una serie di procedure dirette ad analizzare e far fronte all'evento e, per quanto possibile, risolvere o limitare i danni prodotti agli interessati.
La prima di queste procedure è prevista dall'art. 33 del Regolamento. La norma dispone che, qualora si verifichi una violazione dei dati personali il titolare deve, senza ingiustificato ritardo, **notificare** la violazione all'Autorità di controllo.
L'EDPB, nelle sue linee guida in materia, incoraggia i titolari e i responsabili del trattamento ad integrare, nelle valutazioni di loro competenza inerenti al trattamento, anche la pianificazione dei processi per essere in grado di rilevare e contenere tempestivamente una violazione dei dati personali; ciò anche al fine di meglio determinare se è necessario notificare la violazione all'Autorità di controllo competente o informare gli interessati. In tal modo, la notifica all'Autorità di controllo dovrebbe costituire una parte di un più ampio processo di gestione e risposta degli incidenti.
Questo perché, al fine di garantire la sicurezza generale del trattamento, la capacità di prevenire una violazione o, qualora questa si verifichi comunque, di reagire tempestivamente è un elemento chiave di qualsiasi politica di sicurezza.
La notifica della violazione ha lo scopo di informare l'Autorità di controllo dell'accaduto affinché questa possa prendere i provvedimenti più opportuni. Questo vuol dire, innanzitutto, che anche l'Autorità di controllo svolgerà una propria valutazione dell'evento in corso e degli impatti sugli interessati e potrà così fornire supporto e indicazioni al titolare. In un secondo momento ciò potrebbe determinare anche l'avvio di un procedimento istruttorio diretto a valutare le eventuali responsabilità del titolare e in che misura l'evento dannoso sia a lui imputabile. Nel caso di responsabilità tale da comportare il ricorso a sanzioni amministrative, l'Autorità di controllo potrà comunque tener conto, al momento di determinare l'ammontare della sanzione pecuniaria, della collaborazione del titolare e del fatto che la violazione è stata da questo correttamente notificata (art. 83, par. 2, lett. h) del RGPD).
Il fattore tempo è uno degli elementi che contribuisce ad una corretta gestione della violazione e limitazione dei danni. Infatti, se non affrontata in modo adeguato e tempestivo, una violazione dei dati personali può aggravare i danni, materiali o immateriali, alle persone fisiche o determinare una perdita del controllo dei dati non più recuperabile.
Pertanto, non appena venuto a conoscenza della violazione, il titolare del trattamento dovrebbe notificare la stessa all'Autorità di controllo. A tal fine, l'art. 33 del Regolamento prescrive di notificare la violazione entro un termine tendenzialmente breve, ossia 72 ore dal momento in cui il titolare ne è venuto a conoscenza.
Il titolare è considerato "**a conoscenza**" della violazione nel momento in cui ha un ragionevole grado di certezza che si sia verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali. Chiaramente, quando questo avvenga esattamente dipenderà dalle circostanze della specifica violazione.

È importante instaurare il prima possibile un canale di comunicazione con l'Autorità di controllo e tenerla costantemente aggiornata affinché questa possa a sua volta attivarsi. Nulla impedisce, però, al titolare di integrare o, meglio, specificare successivamente la notifica.
Le notifiche effettuate oltre il termine delle 72 ore devono essere accompagnate dai motivi del ritardo. Ciò consentirà all'Autorità di verificare se tale ritardo sia giustificabile alla luce della particolare natura e gravità della violazione.
L'obbligo della notifica all'Autorità di controllo deve essere adempiuto a meno che sia improbabile che la violazione dei dati presenti un rischio per i diritti e le libertà delle persone fisiche. Ne seguirà che vanno notificate unicamente le violazioni di dati personali che possono avere **effetti avversi sugli individui**, causando danni fisici, materiali o immateriali. Per esempio, quando dalla violazione deriva la perdita del controllo sui propri dati, la limitazione di alcuni diritti, la discriminazione, il furto d'identità o il rischio di frode, la perdita di riservatezza dei dati personali protetti dal segreto professionale, una perdita finanziaria, un danno alla reputazione e qualsiasi altro significativo svantaggio economico o sociale.
Nella pratica non è comunque agevole stabilire quando da una violazione di sicurezza sia improbabile che derivi un rischio per le persone coinvolte e si tratta di casi comunque isolati o non troppo frequenti. Per esempio, una violazione potrebbe non produrre rischi quando i dati personali sono stati resi sostanzialmente incomprensibili – perché opportunamente crittografati – a soggetti non autorizzati e degli stessi dati il titolare ne abbia una copia o un *backup*; in tali casi il titolare potrebbe non dover effettuare la notifica all'Autorità di controllo. Se questo è vero in astratto, bisognerebbe comunque tener conto che le condizioni e il contesto della violazione potrebbe cambiare e con esso anche il livello di rischio probabile. Ad esempio, se in seguito si scopre che la chiave usata per crittografare i dati è compromessa.
Ben più ricorrente è quindi l'ipotesi in cui la notifica della violazione sia necessaria e, in questo caso, la notifica deve contenere (almeno) tutti gli elementi necessari per descrivere la natura, le circostanze e le probabili conseguenze della violazione dei dati personali, ivi comprese le categorie e il numero approssimativo di interessati coinvolti, oltre che il nome e i dati di contatto del responsabile della protezione dei dati, nonché le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione o per attenuarne i possibili effetti negativi.
Tali elementi risulteranno necessari per verificare se siano state messe in atto tutte le misure tecnologiche e organizzative necessarie a proteggere i dati personali o attenuarne i rischi e, in ultima misura, a valutare gli impatti della violazione (considerando 87 RGPD).
Affinché il titolare possa prontamente assolvere alla notifica, è inoltre imposto al **responsabile del trattamento** che viene a conoscenza di una eventuale violazione di informare tempestivamente il titolare (art. 33, par. 2, RGPD). Si tratta di uno specifico obbligo che il Regolamento pone in capo al responsabile sicché, sebbene il titolare mantenga la responsabilità generale sul trattamento, il responsabile riveste comunque un ruolo importante al fine di consentire al titolare di rispettare i propri

obblighi. Inoltre, se in linea di principio il titolare del trattamento dovrebbe essere considerato "a conoscenza" della violazione una volta che il responsabile lo ha informato della violazione in corso o avvenuta, bisogna anche tener a mente che il Regolamento non impone al responsabile di valutare l'entità del rischio derivante da tale violazione ma spetterà sempre al titolare, una volta informato, valutarne l'entità e l'integrazione dei presupposti per la notifica all'Autorità di controllo.
Rilevante sarà, inoltre, anche la partecipazione del **Responsabile per la Protezione dei Dati** (RPD), il cui nominativo e contatto dovrà essere fornito all'Autorità di controllo in sede di notifica.
In considerazione dei suoi compiti e competenze, l'RPD ben può assistere il titolare nella prevenzione di una violazione fornendo consulenza e monitorando il trattamento e lo stesso può fare durante una violazione e qualsiasi successiva indagine da parte dell'Autorità di controllo. È quindi raccomandabile che l'RPD venga tempestivamente informato dell'esistenza di una violazione e sia coinvolto durante tutto il processo di gestione e notifica.
Il titolare del trattamento dovrà, inoltre, a prescindere dalla notifica all'Autorità di controllo e in base al principio di *accountability*, documentare tutte le violazioni dei dati personali, ad esempio predisponendo un apposito registro. Dunque, indipendentemente dal fatto che una violazione debba o meno essere notificata all'Autorità di controllo, il titolare deve conservare la documentazione di tutte le violazioni avvenute. Tale documentazione consente all'Autorità di effettuare eventuali verifiche sul rispetto della normativa.

PNRR e notifica semplificata

Durante la redazione di questo manuale è stato pubblicato in Gazzetta Ufficiale il decreto-legge 19 febbraio 2026, n. 19, recante "Ulteriori disposizioni urgenti per l'attuazione del Piano nazionale di ripresa e resilienza (PNRR) e in materia di politiche di coesione" che contiene articoli di interesse in materia di protezione dei dati personali. Quello di maggior rilievo in questa sede è l'articolo 12, comma 1 che novella il Codice introducendo l'art. 2-*quaterdecies*.1 per consentire alle **imprese con meno di cinque dipendenti** di usufruire di **una procedura di notifica delle violazioni specifica.** Tale notifica dovrà essere definita dal Garante per la protezione dei dati personali, con proprio provvedimento, e prevederà strumenti di autovalutazione guidata e un canale di assistenza semplificata per supportare i soggetti nell'adempimento dell'obbligo di notifica.

Notifica in materia di *cybersicurezza*

Come si avrà modo di approfondire nei prossimi capitoli, anche la normativa in materia di cybersicurezza ha introdotto un sistema di notifica degli incidenti di sicurezza simile a quella del RGPD.
Infatti, nel recepire la Direttiva NIS 2, anche l'art. 25 del d.lgs. 4 settembre 2024, n. 138 impone ai soggetti essenziali e ai soggetti importanti di notificare, senza ingiustificato ritardo, al CSIRT Italia ogni incidente che ha un impatto significativo sulla fornitura dei loro servizi.

La proposta di regolamento *Digital Omnibus*

L'art. 3, par. 8 della proposta di Digital Omnibus interviene sulla notifica delle violazioni dei dati personali all'autorità di controllo con modifiche strutturali e importanti.
Innanzitutto, si propone la modifica del primo paragrafo e l'inserimento di un paragrafo 1-*bis* nonché dei nuovi paragrafi 6 e 7.
Così facendo, l'intento è quello di notificare solo le violazioni che risulteranno "suscettibili di presentare un rischio elevato" e la notifica andrà fatta non più semplicemente all'autorità competente *ex* art. 55 del RGPD, bensì si dovrà tener conto di dove sia lo stabilimento principale o unico del titolare al fine di individuare la competenza di quella che è definita l'Autorità di controllo capofila, ai sensi degli artt. 55 e 56 RGPD. In altre parole, si estende anche alle ipotesi di *data breach* l'ordinario meccanismo di ripartizione della competenza tra le autorità di controllo europee che va sotto il nome di "**meccanismo dello sportello unico**" (o *One Stop Shop*) disciplinato dai Capi VI e VII del RGPD. In estrema sintesi, l'autorità di controllo capofila è l'autorità dello stabilimento principale o unico nell'UE del titolare o responsabile del trattamento, alla quale viene trasferita la competenza da tutte le altre autorità di controllo (definite, in questo caso, "autorità interessate") per quanto riguarda i "trattamenti transfrontalieri" di dati personali svolti da quel titolare o responsabile.
Si allunga inoltre il termine per notificare la violazione all'autorità di controllo che passerebbe così dalle attuali 72 alle 96 ore.
Soprattutto, la modifica di più grande impatto, che va a toccare non solo la normativa sulla *data protection* ma anche quella sulla *cybersecurity,* è il fatto che la notifica andrà eseguita non direttamente alle singole autorità di controllo nazional bensì tramite il **punto di accesso unico** (***Single-Entry Point***) istituito a norma dell'introducendo art. 23-*bis* della direttiva UE 2022/2555, ossia la Direttiva NIS 2.
Il punto di accesso unico è considerato una soluzione centrale per razionalizzare l'obbligo di segnalazione degli incidenti applicando il principio del "*report once, share many*" (segnala una volta, condividi con molti). L'obiettivo è ridurre gli oneri amministrativi per le imprese che, a fronte di un unico evento, si trovano oggi a dover inviare notifiche separate a diverse autorità nazionali ed europee.
Ecco perché la modifica coinvolgerà non solo la notifica di *data breach* ai sensi del RGPD ma anche le notifiche di incidenti gravi da parte delle entità soggette a **NIS2** (settori essenziali), **DORA** (settore finanziario), **eIDAS** (servizi fiduciari).
A tal fine, il Comitato europeo per la protezione dei dati (EDPB) ha il compito di proporre un **modello comune di notifica** che la Commissione adotterà tramite atto di esecuzione, garantendo uniformità in tutta l'Unione. L'Agenzia dell'Unione europea per la cibersicurezza (ENISA) sarà poi incaricata di sviluppare e mantenere la piattaforma, nonché di garantire che il sistema sia sicuro, interoperabile e basato su standard leggibili meccanicamente.

4. Comunicazione agli interessati

La seconda procedura diretta ad analizzare e gestire uno scenario di rischio in corso e la violazione dei dati personali è prevista dall'art. 34 del Regolamento.