PROCEDURA INTERNA SULLA CORRETTA GESTIONE DI UNA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

PALERMO ENERGIA S.p.A., (C. f. e P. IVA: 04939480820) (infra "PALERMO ENERGIA"), in persona del suo legale rappresentante pro tempore, con sede legale in Palermo, via Maqueda, 100, intende illustrare – in ossequio al combinato disposto tra gli artt. 5 paragrafo 2), 24 paragrafo 2), 32 paragrafo 1) e Considerando n. 87) del GDPR – il formale processo (interno) di gestione[1] di una "violazione dei dati personali" (data breach) ex art. 4 n. 12)[2] del GDPR.

1. Violazione dei dati personali: definizione e tipologie.

1.1. Al fine di porre rimedio a una violazione dei dati personali, occorre, innanzitutto, conoscerla: a tal fine, si precisa che l'art. 4 n. 12) del GDPR la definisce testualmente come "**la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati**"[3]: in altri termini, un data breach rappresenta una (macro) tipologia di incidente di sicurezza[4], in conseguenza del quale non si è più in grado di garantire l'osservanza dei principi relativi al trattamento dei dati personali di cui all'art. 5 del GDPR.

1.2. Nel dettaglio, una violazione dei dati personali[5] può essere classificata in base ai seguenti tre principi:

- **violazione della riservatezza**: si verifica in caso di divulgazione dei dati personali o accesso agli stessi in modo non autorizzato o accidentale;
- **violazione dell'integrità**: si verifica in caso di modifica non autorizzata o accidentale dei dati personali;
- **violazione della disponibilità**: si verifica in caso di perdita, accesso o distruzione accidentale o non autorizzata di dati personali: essa può essere temporale (ossia, i dati personali sono recuperabili, ma è necessario un certo periodo di tempo) ovvero permanente (ossia, i dati personali non possono essere recuperati).
  Un incidente di sicurezza che determina l'indisponibilità dei dati personali per un certo periodo di tempo può costituire una violazione in quanto la mancanza di accesso ai dati può avere un impatto significativo sui diritti e sulle libertà delle persone fisiche: es. l'indisponibilità, anche solo temporanea, di dati medici (critici) di pazienti di un ospedale potrebbe presentare un rischio per i diritti e libertà delle persone interessate in quanto potrebbe comportare l'annullamento di operazioni e mettere a rischio la vita dei pazienti; all'opposto, l'indisponibilità dei dati personali dovuta allo svolgimento di un intervento di manutenzione (programmato) del sistema non costituisce un data breach.

Si osserva che, a seconda dei casi, un data breach può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse.

---

[1] Tale processo si è fondato, in via principale, sull'analisi della seguente documentazione: Provvedimento del Garante Privacy italiano n. 157 del 30.7.2019; Linee Guida n. 250/2018 del WP Art. 29 (ora, EDPB); "Recommendations for a methodology of the assessment of severity of personal data breaches" a firma dell'ENISA, 2013; Linee Guida n. 1/2022 del 14.12.2021 dell'EDPB.

[2] Giova osservare che la predisposizione di una policy per la gestione di un data breach (e la formazione del personale che ne deve accompagnare l'effettiva attuazione) – sebbene non sia un adempimento espressamente indicato all'interno del GDPR, ma comunque desumibile da almeno due disposizioni (ossia, l'art. 24 paragrafo 2) ed il Considerando n. 87) del GDPR) – costituisce una misura organizzativa pressoché indispensabile rispetto a una tale emergenza, connotata da carattere espansivo, da tempi di risposta estremamente contingentati e, infine, dall'esigenza di agire, in parallelo, su più fronti (anziché in sequenza). Nello specifico, tale processo è teso a rilevare e limitare, in modo tempestivo, gli effetti di una violazione di dati personali, valutare il rischio per le persone fisiche coinvolte e, da ultimo, stabilire se sia (o meno) necessario effettuare la notifica all'Autorità di Controllo competente ed effettuare la comunicazione di tale evento alle persone fisiche interessate: a tal riguardo, si precisa che un aspetto fondamentale di qualsiasi politica di sicurezza dei dati è rappresentato dalla capacità, ove possibile, di prevenire una violazione e, laddove essa si verifichi ciò nonostante, di reagire tempestivamente.

[3] Il significato di "distruzione" dei dati personali si verifica quando gli stessi non esistono più o non esistono più in una forma che sia di qualche utilità per il Titolare (o co-Titolare) del trattamento; si verifica un "danno" quando i dati personali sono stati modificati, corrotti o non sono più completi; con "perdita" dei dati personali si dovrebbe, invece, intendere il caso in cui i dati potrebbero comunque esistere, ma il Titolare (o co-Titolare) potrebbe averne perso il controllo o l'accesso, oppure non averli più in possesso; infine, un trattamento non autorizzato o illecito può includere la divulgazione dei dati personali a (o l'accesso da parte di) destinatari non autorizzati a ricevere (o ad accedere a) i dati oppure qualsiasi altra forma di trattamento in violazione della normativa (nazionale e comunitaria) sulla protezione dei dati personali.

[4] Cfr. D.Lgs. n. 65 del 18.5.2018, art. 3 comma 1) lettera l): "incidente": "ogni evento con un reale effetto pregiudizievole per la sicurezza della rete e dei sistemi informativi".

[5] Cfr., in via analogica, il D.P.C.M. n. 81 del 14.4.2021: esempi di incidenti di sicurezza (che possono determinare una violazione dei dati personali): perdita e/o compromissione di chiavi di cifratura e/o certificati; perdita e/o compromissione di credenziali utenti; impossibilità di accesso fisico alle componenti; privilege escalation: impiego non autorizzato di tecniche, condotte dall'interno della rete, utili ad ottenere permessi di livello superiore; persistence: impiego non autorizzato di tecniche, condotte dall'interno della rete, utili ad ottenere la persistenza di un codice malevolo o d'accesso; defence evasion: impiego non autorizzato di tecniche attraverso cui sono stati effettivamente elusi i sistemi di sicurezza; command and control: comunicazioni non autorizzate verso l'esterno della rete; discovery: impiego non autorizzato di tecniche, condotte dall'interno della rete, utili a effettuare attività di ricognizione; credential access: impiego non autorizzato di tecniche utili ad acquisire, dall'interno della rete, credenziali valide per l'autenticazione alle risorse di rete ovvero rinvenimento di copie non autorizzate; lateral movement: impiego non autorizzato di tecniche utili ad accedere o eseguire un codice tra risorse interne della rete; collection: impiego non autorizzato di tecniche utili a raccogliere, dall'interno della rete, dati di interesse di terze parti ovvero rinvenimento di copie non autorizzate; esfiltrazione: impiego non autorizzato di tecniche utili ad esfiltrare dati dall'interno della rete verso risorse esterne; inhibit response function: impiego non autorizzato di tecniche utili a inibire l'intervento delle funzioni di sicurezza, di protezione e di "quality assurance" dei sistemi di controllo industriale, predisposte per rispondere a un disservizio o a uno stato anomalo; impair process control: impiego non autorizzato di tecniche utili a manipolare, disabilitare o danneggiare i processi di controllo fisico di sistemi di controllo industriale; impact: impiego non autorizzato di tecniche utili a manipolare, degradare, interrompere o distruggere i sistemi, i servizi o i dati (es. denial of service/distributed denial of service).

2. Data breach: analisi del rischio (probabile e/o elevato) dei diritti e delle libertà di un soggetto interessato.

2.1. Al fine di orientarsi circa l'esecuzione di tale attività di risk assessment, è necessario, innanzitutto, evidenziare quanto prescrive espressamente, in merito, il GDPR, rispettivamente agli artt. 33 e 34 paragrafo 1):

- L'art. 33 paragrafo 1) del GDPR stabilisce espressamente che: "In caso di violazione dei dati personali, il titolare del trattamento **notifica** la violazione **all'autorità di controllo** competente […] senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, **a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche**. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo";
- L'art. 34 paragrafo 1) del GDPR aggiunge che: "Quando la violazione dei dati personali è suscettibile di presentare un **rischio elevato** per i diritti e libertà delle persone fisiche, il titolare del trattamento **comunica** la violazione **all'interessato** senza ingiustificato ritardo".

2.2. L'analisi del relativo rischio deve avere, dunque, come esito la determinazione dei seguenti due parametri:

I. la probabilità (likelihood) delle conseguenze del data breach per il soggetto interessato, al fine così, in caso di esito positivo, di procedere alla notifica di tale evento al Garante Privacy competente;
II. la gravità (severity) delle conseguenze del data breach nei confronti del soggetto interessato, al fine così, in caso di esito positivo, di effettuare la comunicazione della violazione de quo al relativo interessato coinvolto[6].

2.3. Nello specifico, le conseguenze pregiudizievoli che potrebbero derivare dal data breach, e che vanno, perciò, valutate in termini di probabilità e di gravità sono quelle elencate nei Considerando n. 75)[7] e 85)[8] del GDPR: tale valutazione (oggettiva) del rischio[9] va, tuttavia, condotta tenendo conto dei seguenti fattori, illustrati all'interno delle Linee Guida n. 250/2018 a firma del Gruppo di Lavoro Art. 29 per la protezione dei dati (infra "WP 29"; ora, EDPB):

- Tipologia della violazione: tale aspetto può influire sul livello di rischio presentato per le persone fisiche (i.e.: una violazione della riservatezza che ha portato alla divulgazione di informazioni mediche a soggetti non autorizzati può avere conseguenze diverse per una persona fisica rispetto a una violazione in cui i dettagli medici di una persona fisica sono stati persi e non sono più disponibili);
- Natura, carattere (sensibile) e volume dei dati personali: com'è noto, un elemento fondamentale della valutazione del rischio sono il tipo e il carattere sensibile dei dati personali che sono stati compromessi dalla violazione; solitamente più i dati sono sensibili, maggiore è il rischio di danni per le persone interessate; tuttavia, si dovrebbero prendere in considerazione anche altri dati personali che potrebbero già essere disponibili sull'interessato (i.e. è improbabile che la divulgazione del nome e dell'indirizzo di una persona fisica in circostanze ordinarie causi un danno sostanziale; violazioni relative ai dati sulla salute, documenti d'identità o dati finanziari come i dettagli di una carta di credito possono causare danni di per sé, ma se tali informazioni fossero usate congiuntamente si potrebbe avere un'usurpazione d'identità);
- Facilità di identificazione della persona fisica: facilità con cui un soggetto che può accedere ai dati personali compromessi riesce ad identificare persone specifiche o ad abbinare i dati con altre informazioni per identificare persone fisiche;
- Gravità delle conseguenze per la persona fisica: a tal fine, il fatto che il Titolare (o co-Titolare) del trattamento sappia (o meno) che i dati personali sono posseduti da persone le cui intenzioni sono sconosciute o potenzialmente dannose può incidere sul livello di rischio potenziale;
- Caratteristiche (particolari) del soggetto interessato (i.e.: sussiste un rischio più elevato di danno se un data breach riguarda dati personali relativi a minori o ad altre persone fisiche vulnerabili);
- Caratteristiche (particolari) del Titolare (o co-Titolare) del trattamento: la natura ed il ruolo di tale soggetto (e delle sue attività) può influire sul livello di rischio per le persone fisiche a seguito di una violazione (i.e.: un'organizzazione medica

---

[6] La ratio primaria dei due istituti (notificazione e comunicazione) consiste nella necessità di apprestare un fronte composito di contenimento dell'emergenza e delle sue conseguenze, coinvolgendo tutti i soggetti che, ciascuno secondo le rispettive competenze e possibilità, si trovano in condizione di affrontarne specifici profili e limitarne la portata espansiva; del resto, come chiarito dal Considerando n. 89) del GDPR, il Legislatore europeo ha ritenuto "opportuno abolire […] obblighi generali e indiscriminati di notifica" vigenti in passato e "sostituirli con meccanismi e procedure efficaci che si concentrino piuttosto su quei tipi di trattamenti che potenzialmente presentano un rischio elevato per i diritti e le libertà delle persone fisiche, per loro natura, ambito di applicazione, contesto e finalità".

[7] "I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati".

[8] "Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata..."

[9] Va osservato che la valutazione del rischio per i diritti e le libertà delle persone fisiche a seguito di un data breach esamina il rischio in maniera differente rispetto alla valutazione d'impatto sulla protezione dei dati (DPIA) ex art. 35 del GDPR.

tratterà categorie particolari di dati personali, il che significa che vi è una minaccia maggiore per le persone fisiche nel caso in cui i loro dati personali vengano violati);

- Numero di persone fisiche interessate: di norma, maggiore è il numero delle persone fisiche interessate, maggiore è l'impatto che una violazione può avere; tuttavia, si noti che un data breach può avere ripercussioni gravi anche su una sola persona fisica, a seconda della natura dei dati personali e del contesto nel quale i dati sono stati compromessi.

2.4. Orbene, dei due esiti anzidetti, ossia gravità e probabilità, il secondo è autonomamente sufficiente ad innescare l'obbligo di notificazione al Garante Privacy competente, e dunque prescinde da una valutazione in ordine alla severità delle conseguenze pregiudizievoli per il soggetto interessato; ciò significa, pertanto, che il Titolare (o co-Titolare) del trattamento, nel (compresso) periodo di reazione ad un data breach, deve, innanzitutto, concentrare le sue risorse di analisi sulla determinazione della probabilità del rischio, ed immediatamente dopo, in caso appunto di rischio probabile, anche sulla comprensione della sua gravità.

3. Notifica del data breach al Garante Privacy competente.

3.1. Come sopra anticipato, il GDPR impone al Titolare (o co-Titolare) del trattamento di notificare una violazione dei dati personali **senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza**, nel caso in cui l'esito del relativo risk assessment (descritto al precedente art. 2) abbia rilevato una probabilità di rischio per i diritti e le libertà dei soggetti interessati coinvolti nell'evento in parola.

Nello specifico, tale termine è da intendersi come decorrente dal momento in cui il Titolare (o co-Titolare) del trattamento è ragionevolmente certo che si è verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali: dunque, il Titolare (o co-Titolare) del trattamento è tenuto a prendere le misure necessarie per assicurarsi di venire "a conoscenza" di eventuali data breach in maniera tempestiva in modo da poter adottare le misure appropriate.

3.2. Quando il Titolare (o co-Titolare) del trattamento notifica una violazione al Garante Privacy, l'art. 33 paragrafo 3) del GDPR stabilisce che essa deve almeno contenere le seguenti informazioni: a) descrizione della natura della violazione dei dati personali, ivi incluso, ove possibile, le categorie e il numero (approssimativo) dei soggetti interessati, nonché le categorie e il numero (approssimativo) dei dati personali[10]; b) comunicazione del nome e dei dati di contatto del DPO o di un altro punto di contatto presso cui il Garante Privacy può ottenere informazioni; c) descrizione delle probabili conseguenze della violazione; d) descrizione delle misure adottate o di cui si propone l'attuazione per porre rimedio alla violazione dei dati occorsa ed eventualmente per attenuare i possibili effetti negativi.

La notifica deve essere inviata al Garante Privacy tramite l'apposita procedura telematica introdotta con Provvedimento del 21.5.2021 a firma del Garante Privacy (ed operativa dal 1.7.2021)

3.3. **Notifica a fasi**: a seconda della natura della violazione, il Titolare (o co-Titolare) del trattamento può avere la necessità di effettuare ulteriori accertamenti per stabilire tutti i fatti pertinenti al data breach: a tal fine, l'art. 33 paragrafo 4) del GDPR acconsente alla notifica per fasi ("Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo"). E' opportuno, inoltre, precisare che se, dopo la notifica iniziale, una successiva indagine dimostra che l'incidente di sicurezza è stato contenuto e che non si è verificata alcuna violazione, il Titolare (o co-Titolare) del trattamento può informare il Garante Privacy; tali informazioni possono, quindi, essere aggiunte alle informazioni già fornite al Garante medesimo, e l'incidente può essere, di conseguenza, registrato come un evento che non costituisce una violazione.

3.4. **Notifica in ritardo**: l'art. 33 paragrafo 1) del GDPR chiarisce che, qualora non sia effettuata entro 72 ore, la notifica al Garante Privacy deve essere corredata dei motivi del ritardo.

3.5. **Notifica cumulativa**: al fine di evitare che il processo diventi eccessivamente oneroso, il Titolare (o co-Titolare) del trattamento può presentare una notifica cumulativa che rappresenta tutte le violazioni in questione, a condizione che riguardino la medesima tipologia di dati personali e che questi siano stati violati nel medesimo modo e in un lasso di tempo relativamente breve.

4. Comunicazione al soggetto interessato.

4.1. Come anticipato, può accedere che, laddove la violazione abbia prodotto un rischio elevato[11] per i diritti e le libertà del soggetto interessato (aspetto da verificarsi come risultato del risk assessment meglio descritto al precedente art. 2), il Titolare (o co-Titolare) del trattamento è tenuto ad effettuare, **senza ingiustificato ritardo** (ossia, il prima possibile), la comunicazione del data breach a ciascun soggetto interessato coinvolto[12].

L'obiettivo principale della comunicazione agli interessati consiste nel fornire loro informazioni specifiche sulle misure che questi possono prendere per proteggersi da eventuali conseguenze negative della violazione di specie.

4.2. In ossequio al combinato disposto tra l'art. 33 paragrafo 2) e l'art. 34 paragrafo 2) del GDPR, il Titolare (o co-Titolare) del trattamento deve fornire, con un linguaggio semplice e chiaro, almeno le seguenti informazioni: a) una descrizione della natura della violazione; b) il nome ed i dati di contatto del DPO o di un altro punto di contatto; c) una descrizione delle (probabili) conseguenze della violazione; d) una descrizione delle misure adottate o di cui si propone l'adozione, da parte del Titolare (o co-Titolare) del trattamento per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

4.3. In linea di principio, la violazione dovrebbe essere comunicata direttamente agli interessati coinvolti, a meno che ciò richieda uno sforzo sproporzionato: in tal caso, si può procedere a una comunicazione pubblica o a una misura simile che permetta di informare gli interessati con analoga efficacia.

---

[10] Il fatto che non siano disponibili informazioni precise (es. il numero esatto di interessati coinvolti) non deve costituire un ostacolo alla notifica tempestiva della violazione.

[11] La gravità di una violazione è definita come la stima dell'entità del potenziale impatto sugli individui derivante dalla violazione dei dati.

[12] La soglia per la comunicazione delle violazioni alle persone fisiche è, quindi, più elevata rispetto a quella della notifica al competente Garante Privacy: pertanto, non tutte le violazioni dovranno essere comunicate ai soggetti interessati.

Nel comunicare una violazione si devono utilizzare messaggi dedicati che non devono essere inviati insieme ad altre informazioni (es. aggiornamenti regolari; newsletter; messaggi standard); altresì, si precisa che deve essere scelto un mezzo che massimizzi la possibilità di comunicare correttamente le informazioni a tutte le persone interessate.

4.4. **Rischio elevato**: in via generale, tale rischio sussiste quando la violazione può comportare un danno fisico, materiale o immateriale per le persone fisiche i cui dati sono stati violati (es.: discriminazione; furto o usurpazione d'identità; perdite finanziarie; pregiudizio alla reputazione).

A tal fine, un utile strumento è, senz'altro, rappresentato dalla metodologia di valutazione predisposta dall'ENISA all'interno del documento intitolato "Recommendations for a methodology of the assessment of severity of personal data breaches"[13].

Per semplicità, si illustra, di seguito, una (estrema) sintesi della tabella di valutazione della gravità di una violazione dei dati, predisposta dall'ENISA all'interno del citato documento:

Gravità BASSA	Il soggetto interessato potrebbe incontrare alcuni inconvenienti, superabili senza problemi (es. tempo speso per reinserire le informazioni; fastidi; irritazioni).
Gravità MEDIA	Il soggetto interessato potrebbe incontrare disagi significativi che sarà in grado di superare nonostante alcune difficoltà (es. costi aggiuntivi; rifiuto di accesso a servizi aziendali; mancanza di comprensione; stress; disturbi fisici minori).
Gravità ALTA	Il soggetto interessato potrebbe incontrare conseguenze significative che dovrebbe essere in grado di superare anche se con gravi difficoltà (es. appropriazione indebita di fondi; inserimento in una black list; danni alla proprietà; perdita del lavoro; mandato di comparizione; peggioramento della salute).
Gravità MOLTO ALTA	Il soggetto interessato potrebbe incontrare un danno significativo o irreversibile (es. difficoltà finanziarie, come debiti ingenti; incapacità lavorativa; disturbi psicologici o fisici a lungo termine; morte).

5. Co-Titolare del trattamento.

5.1. Si precisa che, nel rispetto peraltro dell'art. 26 del GDPR, l'eventuale accordo di co-titolarità deve includere, al suo interno, disposizioni che stabiliscano quale Titolare del trattamento assumerà il comando ovvero sarà responsabile del rispetto degli obblighi di notifica delle violazioni.

6. Responsabile del trattamento.

6.1. Sebbene il Titolare (o co-Titolare) del trattamento conservi la responsabilità generale per la protezione dei dati personali, il Responsabile del trattamento svolge un ruolo importante nel consentire al Titolare (o co-Titolare) di adempiere ai propri obblighi, segnatamente in materia di notifica (e/o comunicazione) di un data breach.

A tal riguardo, si ricorda che l'art. 33 paragrafo 2) del GDPR chiarisce che se il Titolare (o co-Titolare) del trattamento ricorre a un Responsabile del trattamento e quest'ultimo viene a conoscenza di una violazione dei dati personali che sta trattando per conto del Titolare (o co-Titolare) del trattamento, il Responsabile del trattamento deve notificarla al Titolare (o co-Titolare) del trattamento "senza ingiustificato ritardo".

Va notato che il Responsabile del trattamento non è tenuto a valutare la probabilità del rischio derivante dal data breach prima di notificarlo al Titolare (o co-Titolare) del trattamento; il primo deve, infatti, soltanto stabilire se si è verificata una violazione e, quindi, notificarla al Titolare del trattamento.

6.2. Il Responsabile del trattamento può effettuare la notifica per conto del Titolare (o co-Titolare) del trattamento qualora quest'ultimo gli abbia concesso l'opportuna autorizzazione, e ciò faccia parte degli accordi contrattuali tra il Titolare (o co-Titolare) del trattamento ed il Responsabile del trattamento; tuttavia, è importante osservare che la responsabilità legale della notifica rimane in capo al Titolare (o co-Titolare) del trattamento.

[13] Tale documento non è da intendersi come uno strumento esaustivo e generale, ma i suoi esiti vanno piuttosto assunti quali indicazioni operative; pregio principale del metodo è quello di fornire una metrica esatta della gravità del rischio secondo una logica verificabile e un'impostazione il più possibile algebrica. La non perfetta sovrapposizione del metodo in commento con l'assetto normativo suggerisce di evitare applicazioni automatiche, quanto piuttosto di farne un utilizzo accorto e prudente, assistito da opportune correzioni critiche che recepiscano esigenze di conformità anche squisitamente giuridiche.

7. Documentazione del data breach occorso.

7.1. Indipendentemente dal fatto che una violazione debba (o meno) essere notificata al competente Garante Privacy (ed eventualmente comunicata ai soggetti interessati coinvolti in essa), il Titolare (o co-Titolare) del trattamento deve conservare la documentazione di tutte le violazioni.

Come richiesto dall'art. 33 paragrafo 5) del GDPR, il Titolare (o co-Titolare) del trattamento è tenuto a registrare i dettagli relativi alla violazione, ivi comprese le cause, i fatti, i dati personali, gli effetti e le conseguenze della violazione, i relativi provvedimenti adottati per porvi rimedio nonché, infine, il ragionamento alla base delle decisioni prese in risposta ad una violazione (es. se un data breach non viene notificato, è opportuno documentare una giustificazione di tale decisione).

8. Esempi di data breach, riguardo i quali, a parere dell'EDPB, risulta necessaria o meno la notifica al Garante Privacy e/o la comunicazione a ciascun soggetto interessato coinvolto nell'evento.

Si illustrano, di seguito, i (macro) data breach che possono risultare di maggiore utilità pratica, tratti dalle recenti Linee Guida n. 1/2022 a firma dell'EDPB:

i. **Ransomware**

Ipotesi (1): l'attacco informatico ha riguardato i dati personali (soggetti ad un regolare back up crittografato a riposo) detenuti da una piccola azienda manifatturiera, senza l'esfiltrazione degli stessi; considerato il back up prontamente disponibile che, pertanto, non ha determinato alcuna conseguenza negativa sul funzionamento quotidiano dell'impresa, l'EDPB ritiene corretto che, in tale ipotesi, non sussiste la necessità né di una notifica all'Autorità di Controllo né, tantomeno, di una comunicazione ai soggetti interessati coinvolti.

Ipotesi (2): l'attacco informatico ha riguardato i dati personali (non soggetti ad alcun back up) detenuti da un'azienda agricola, senza l'esfiltrazione degli stessi; considerata l'assenza di un back up, il ripristino dei dati ha necessitato di diversi giorni lavorativi con conseguenti ritardi nella consegna degli ordini alla relativa clientela: alla luce di ciò, l'EDPB ritiene corretto che, in tale ipotesi, sussiste soltanto la necessità di una notifica all'Autorità di Controllo.

Ipotesi (3): l'attacco informatico ha riguardato i dati personali e i dati personali cd. particolari (soggetti ad un regolare back up) del personale e dei pazienti di un ospedale/struttura sanitaria, senza l'esfiltrazione degli stessi; nonostante il back up presente, l'attività di ripristino è durata un paio di giorni, determinando, di conseguenza, disguidi, rinvii e cancellazioni delle operazioni sanitarie programmate: in ragione di ciò, l'EDPB ritiene corretto che, in tale ipotesi, sussiste la necessità sia di una notifica all'Autorità di Controllo sia di una comunicazione ai soggetti interessati.

Con riguardo alla descritta (macro) tipologia di violazione informatica, l'EDPB ha individuato una serie di misure di mitigazione tecnico/organizzative, così sintetizzate: firmware, da aggiornare costantemente; procedura di segmentazione ed isolamento dei dati e delle reti; back up aggiornato, sicuro e (periodicamente) testato; firewall appropriato, aggiornato, efficace ed integrato; sistema di rilevamento e prevenzione delle intrusioni; crittografia forte; autenticazione a due fattori, ove possibile; test di vulnerabilità e di penetrazione su base regolare.

ii. **Fonte di rischio umano (interna)**

Ipotesi (1): durante il periodo di preavviso, un dipendente di una società ha copiato i dati personali dei clienti dal database aziendale, per poi utilizzarli, dopo poco, al fine di contattarli in nome della nuova società di cui era entrato a far parte: in tal caso, l'EDPB ritiene corretto che sussiste soltanto la necessità di una notifica all'Autorità di Controllo.

Ipotesi (2): un agente assicurativo si è accorto di poter accedere, grazie a un bug di sistema, ad una serie di informazioni personali (es. tipologia ed importo dell'assicurazione) relative a clienti non propri: in tal caso, l'EDPB ritiene che non sussista la necessità né di una notifica all'Autorità di Controllo né, tantomeno, di una comunicazione ai soggetti interessati coinvolti.

Con riguardo alla descritta (macro) categoria di data breach, l'EDPB ha individuato una serie di misure di mitigazione tecnico/organizzative, così sintetizzate: realizzazione periodica di programmi di formazione, educazione e sensibilizzazione del personale dipendente circa gli obblighi privacy, la sicurezza (anche informatica) dei dati personali; access control; controllo del flusso dei dati insolito tra il file server e la stazione di lavoro del dipendente.

iii. **Perdita/furto di un dispositivo informatico o di un documento**

Ipotesi (1): durante un accesso illegale all'interno di una struttura per l'infanzia, viene rubato un personale computer, tuttavia criptato e spento al momento dell'effrazione, e i cui dati personali ivi racchiusi erano stati soggetti ad un apposito back up: in tal caso, l'EDPB ritiene che non sussista la necessità nemmeno di una notifica all'Autorità di Controllo.

Ipotesi (2): furto di un dispositivo elettronico contenente i dati personali di (numerosi) clienti, senza che il dispositivo fosse stato oggetto di crittografia, ma tali informazioni personali era state soggette ad un apposito back up: in tal caso, l'EDPB ritiene che sussista la necessità sia di una notifica all'Autorità di Controllo sia di una comunicazione ai soggetti interessati coinvolti.

Con riguardo alla descritta (macro) categoria di data breach, l'EDPB ha individuato una serie di misure di mitigazione tecnico/organizzative, così sintetizzate: crittografia del dispositivo; autenticazione a più fattori; funzionalità, nei confronti dei dispositivi altamente mobili, tesa alla localizzazione, in caso di perdita o smarrimento degli steesi; VPN sicura; access control; evitare di memorizzare informazioni sensibili sui dispositivi mobili.

Palermo, lì 15.4.2024 (data di ultimo aggiornamento).

PALERMO ENERGIA S.p.A.
(in persona del suo legale rappresentante pro tempore)