PROCEDURA PER LA GESTIONE DI UN DATA BREACH AI SENSI DEL REGOLAMENTO EUROPEO 679/2016 IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

(GDPR)

ACQUA srl
Via Carlo De Angeli 3 | 20141 Milano | t +39 02 45485206
info@acquagroup.it | acquagroup.it | P.I.13198000153

INDICE

1) Premessa

La presente procedura è adottata da **Acqua S.r.l** (P.IVA 13198000153) con sede in Milano Via Carlo de Angeli, 3 e tutte le società ad esse collegate (**Booster srl** e **EMG srl**).

Il presente documento si prefigge lo scopo di fornire indicazioni sulle opportune modalità di gestione degli eventuali data breach, nel rispetto della normativa in materia di trattamento dei dati personali, garantendo in particolare l'aderenza ai principi e alle disposizioni contenute nel Regolamento UE 679/2016.
Nell'elaborato si sintetizzano, quindi, le regole per garantire il rispetto dei principi esposti e la sostenibilità tecnica/ organizzativa, nella gestione dei data breach, sotto i diversi aspetti relativi a:

a) Modalità e profili di segnalazione al Titolare;

b) Modalità e profili di segnalazione all'Autorità Garante;

c) Valutazione dell'evento accaduto;

d) Eventuale comunicazione agli interessati.

Il titolare del trattamento, ha nominato quale DPO/RPD Dott. Davide Scapuzzi domiciliato presso lo Studio Legale Russo di Piacenza,(PC), Viale dei Mille,3.

2) Scopo

Lo scopo di questa procedura è di disegnare un flusso per la gestione delle violazioni di dati personali trattati da Acqua S.r.l (e le società ad essa collegate Booster srl e EMG srl) in qualità di Titolare del trattamento (di seguito "Titolare del trattamento").

3) Definizioni

Ai fini della presente procedura vengono riportate le seguenti definizioni:

Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia digitalizzato o meno, centralizzato, decentralizzato o ripartito in modo funzionale o geografico
(art. 4, par. 1, n. 6).

Data Protection Officer: la persona fisica individuata come Responsabile del trattamento come individuato dalla Sezione 4 (artt. 37-39) del Regolamento (UE) n. 2016/679".

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo

come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (art. 4, par. 1, n. 1).

Incaricato del trattamento: "La persona fisica che nell'ambito della struttura aziendale del Titolare è autorizzata a effettuare attività di trattamento di dati personali".
Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento ai sensi dell'art. 28 GDPR (art. 4, par. 1, n. 8).

Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (art. 4, par. 1, n. 7).

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (art. 4, par. 1, n. 2).

Violazione dei dati personali (Data Breach): 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 (art. 4, par. 1, n. 12)

4) Normativa di riferimento

Regolamento UE 679/2016: artt. 33-34, considerando n. 85-88.
Linee guida del Gruppo Articolo 29 sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679 adottate il 3 ottobre 2017 - Versione emendata e adottata in data 6 febbraio 2018.

5) Gestione del data breach per i dati personali di cui Acqua S.r.l. (e le società ad essa collegate Booster srl e EMG srl) è Titolare del trattamento

La presente procedura è stata messa a disposizione di tutti gli incaricati del trattamento mediante comunicazione inviata all'indirizzo di posta elettronica aziendale.

Ai sensi dell'art. 33 del Regolamento (UE) n. 2016/679, il Titolare del trattamento, in caso sia consapevole di una violazione dei Dati personali trattati, è tenuto:

i. a informare il Garante Privacy entro e non oltre le 72 ore successive all'avvenuta conoscenza della violazione (a meno che non sia improbabile che la violazione dei Dati personali presenti un rischio per i diritti e le libertà degli Interessati);

ii. nel caso in cui tale violazione sia suscettibile di comportare un rischio elevato per i diritti e le libertà degli interessati, a informare senza ritardo anche gli stessi Interessati.

A tal fine, Acqua S.r.l. (e le società ad essa collegate Booster srl e EMG srl) – con il presente atto – si dota di una procedura per gli incidenti informatici e agli archivi cartacei che consenta di attivare un apposito processo per la gestione e la notifica di eventuali Data Breach.

Al fine di rendere effettivo il processo di notifica, questa procedura viene resa nota a tutti coloro che nell'ambito del rapporto di lavoro e/o di collaborazione trattano Dati personali del Titolare del trattamento.
È fatto obbligo a ciascun dipendente e collaboratore della Società di segnalare tempestivamente ogni caso di incidente informatico e/o ad archivi cartacei di cui sia venuto a conoscenza e ogni evento che potrebbe potenzialmente condurre ad una violazione di dati personali

6) Incidenti informatici, incidenti agli archivi cartacei, data breach

Il GDPR definisce violazione dei dati personali o Data Breach "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" (art. 4, par. 1, n. 12).

Le indicazioni di cui alla presente sezione della Procedura valgono per qualsiasi tipologia di Incidente (informatico o agli archivi cartacei) da cui possa derivare un Data Breach.

Eventi di Data Breach possono riguardare sia casi cui è connesso un rischio marginale (es. perdita di una chiavetta USB di un dipendente), che casi più critici di furto o perdita di intere basi dati, quali, a titolo esemplificativo, le banche dati gestite da Venis o documenti presenti nei suoi archivi.

Nel caso si verificasse una delle casistiche riportate di seguito, o un analogo scenario, è fondamentale chiedersi se e quale tipo di Dati personali sono coinvolti nell'evento, e, di conseguenza, procedere alla segnalazione dell'Incidente:

i. furto o smarrimento di PC, laptop, smartphone, tablet aziendali contenenti Dati personali;

ii. furto o smarrimento di documenti cartacei contenenti Dati personali;

iii. furto o smarrimento di dispositivi portatili di archiviazione, come chiavette USB e hard disk esterni, contenenti Dati personali;

iv. perdita o modifica irreparabile di archivi contenenti Dati personali in formato cartaceo o digitale (ad esempio, a causa di una errata cancellazione o modifica dai sistemi o dagli archivi digitali aziendali che non possa essere ripristinata attraverso l'uso di un backup);

v. diffusione impropria di Dati personali, per mezzo di:

◦ invio di e-mail contenente Dati personali al destinatario errato;

◦ invio di e-mail con un file contenente Dati personali allegato erroneamente;

◦ esportazione fraudolenta o errata di Dati personali dai sistemi aziendali;

vi. virus o altri attacchi al sistema informatico o alla rete del Titolare;

vii. divulgazione di dati confidenziali a persone non autorizzate;

viii. violazione del sistema informatico effettuate attraverso rete internet;

ix. violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o archivi, contenenti informazioni riservate);

x. richiesta di invio di documenti e file contenenti Dati personali da parte di un esterno che si finge fraudolentemente un collega, collaboratore e/o altro soggetto e conseguente invio allo stesso di tali documenti e file;

xi. segnalazione da parte di un fornitore di un evento di Data Breach sui propri sistemi che ha interessato o potrebbe potenzialmente interessare Dati personali del Titolare del trattamento.

7) Processo di gestione dell'incidente

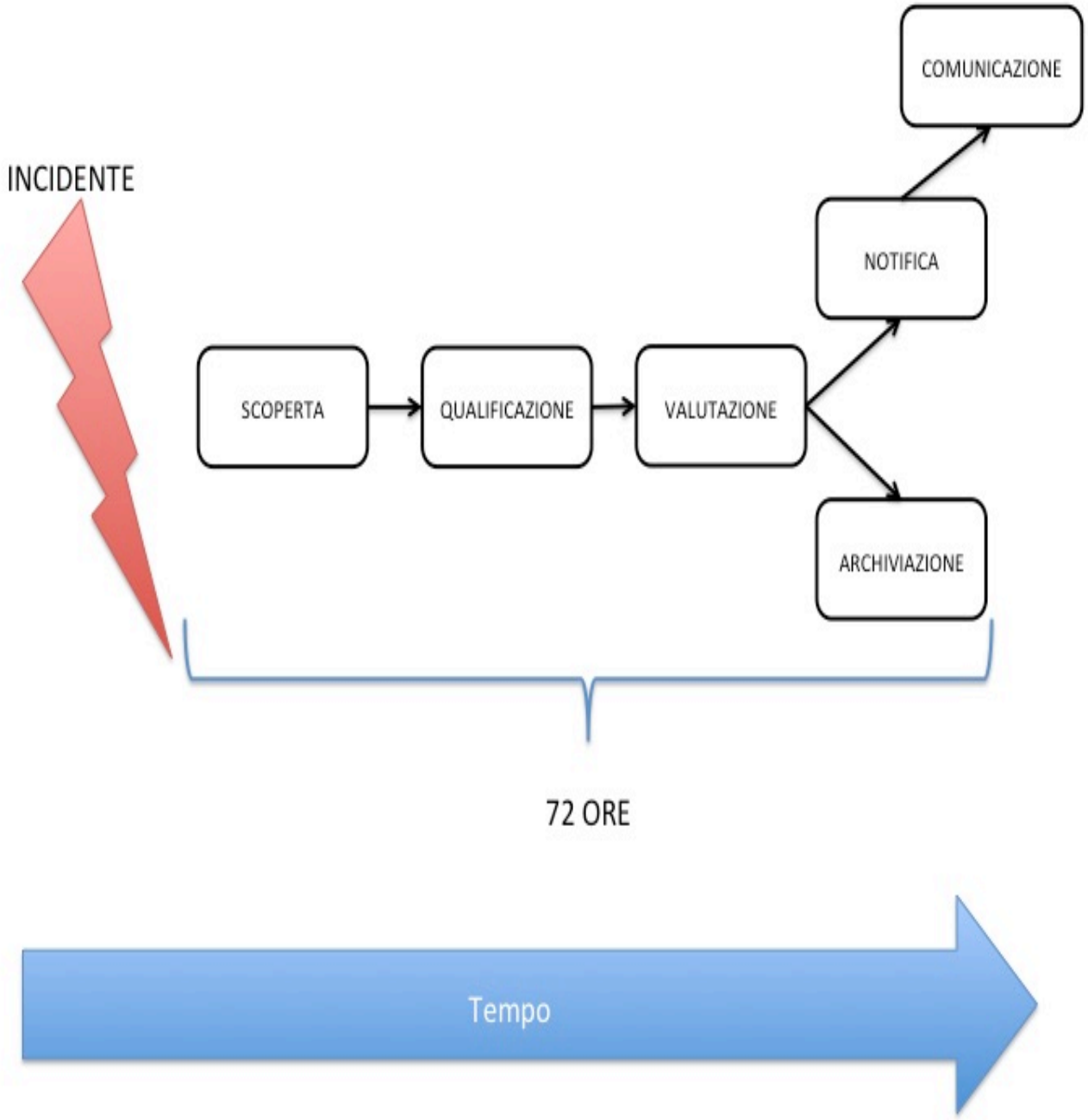
i. Al fine di consentire una gestione efficace e tempestiva delle violazioni dei Dati personali, il Titolare del trattamento adotta un processo strutturato per la gestione dei casi di Incidenti che prevede:

a) Rilevazione e segnalazione dell'Incidente;

b) Analisi dell'Incidente;

c) Registrazione dell'Incidente;

d) Eventuale notifica del Data Breach al Garante da parte del Titolare previa consultazione con il Dpo (entro il massimo di 72 ore).



8) Rilevazione e segnalazione del data breach

La rilevazione e segnalazione dell'Incidente è un obbligo per tutti i dipendenti e/o collaboratori del Titolare del trattamento attraverso i canali per la comunicazione tempestiva degli incidenti (mail e recapiti telefonici).

Nel caso in cui si verifichi uno degli eventi sopradescritti o in tutti gli altri casi in cui il soggetto che tratta dati personali sia consapevole di altri eventi potenzialmente rischiosi per i documenti e gli archivi, è tenuto a informare immediatamente l'Ufficio Tutela Dati.

Una volta ricevuta la segnalazione dell'Incidente, l'Ufficio Tutela Dati provvederà a compilare una scheda su apposito registro informatico la cui struttura è allegata al presente atto (ALLEGATO 1).
Al registro andranno allegate tutte le comunicazioni relative all'incidente (ad es. eventuale denuncia all'autorità giudiziaria, eventuale notifica al Garante Privacy e relativa corrispondenza, eventuali comunicazioni agli interessati, comunicazioni con i dipendenti/collaboratori coinvolti ecc.).

In tale Registro dovranno essere inseriti tutti gli eventi che determinano o configurano anomalie rispetto alla normale gestione dei sistemi informatici e degli archivi cartacei (ad esempio: Virus, perdita di dati, alterazione di dati, attacchi alla rete, furti di credenziali, ecc.).

9) Analisi dell'Incidente

A seguito della rilevazione e/o segnalazione, l'Ufficio Tutela Dati effettua una valutazione al fine di verificare che nell'incidente rilevato siano stati effettivamente violati Dati personali trattati dalla Società.

La suddetta analisi è finalizzata alla raccolta e identificazione delle seguenti informazioni:

i. categorie di Interessati cui i Dati personali violati si riferiscono (ad esempio, utenti, dipendenti, fornitori, etc.);

ii. categorie di Dati personali compromessi (ad esempio, Dati personali, Dati sensibili, Dati giudiziari);

iii. tipologia di incidente: violazione della riservatezza, disponibilità o integrità (ad esempio, accesso non autorizzato, perdita, alterazione, furto, disclosure, distruzione, etc.).

Nell'ambito di tale analisi, l'Ufficio Tutela Dati con il supporto del DPO identifica le azioni di prima risposta da intraprendere nell'immediato per contenere gli impatti dell'incidente.

Nell'ambito dell'analisi dell'incidente, vengono identificate anche le seguenti informazioni:

- identificabilità degli Interessati i cui dati rappresentano l'oggetto della violazione;

- misure di sicurezza tecniche e organizzative che potrebbero aver parzialmente o in toto mitigato gli impatti relativi all'incidente;

- ritardi nella rilevazione dell'incidente;

- numero di individui interessati.

Sulla base dei suddetti parametri, si procede alla valutazione della gravità dell'incidente relativamente ai diritti ed alle libertà degli Interessati, a seconda della natura dei Dati personali (ad esempio, Dati Sensibili e/o Giudiziari), delle misure di sicurezza adottate, della tipologia di interessati (ad esempio, minori o altri soggetti vulnerabili).

10) Risposta e notifica del data breach

La precedente fase di analisi fornisce gli strumenti necessari a identificare e valutare le conseguenze negative e gli impatti causati dall'incidente rilevato.

Nel caso in cui dovesse risultare improbabile che l'incidente presenti rischi per i diritti e le libertà degli interessati, la notifica all'Autorità Garante risulta essere non obbligatoria. Tale valutazione è condivisa con il DPO.

Qualora al contrario dovesse risultare possibile che l'incidente abbia determinato una violazione dei dati che presenti rischi per i diritti e le libertà degli Interessati, l'Ufficio Tutela Dati, con il supporto del DPO, procede a predisporre la notifica all'Autorità Garante secondo il modello allegato al presente atto (ALLEGATO 2).

La notifica viene effettuata all'Autorità Garante entro 72 ore dal momento in cui il Data Breach è stato rilevato.

La suddetta notifica contiene almeno le seguenti informazioni:

i. natura della violazione dei dati personali (disclosure, perdita, alterazione, accesso non autorizzato, etc.);

ii. tipologie di Dati personali violati;

iii. categorie e numero approssimativo di Interessati cui i dati compromessi si riferiscono;

iv. nome e dati di contatto del DPO, che sarà l'interfaccia per Titolare del trattamento nei confronti dell'Autorità di controllo;

v. probabili conseguenze della violazione dei Dati personali;

vi. descrizione delle misure che il Titolare del trattamento ha adottato o è in procinto di adottare al fine di mitigare le conseguenze del Data Breach;

vii. ove la stessa non sia presentata entro 48/72 ore dalla rilevazione, i motivi dell'eventuale ritardo nella comunicazione.

Qualora non sia stato possibile fornire contestualmente tutte le informazioni obbligatorie, l'Ufficio Tutela Dati raccoglie quanto prima le informazioni supplementari e provvede a integrare, senza ritardo, la notifica già inoltrata all'Autorità di Controllo.

11) Modalità di comunicazione agli interessati

Oltre a notificare il Data Breach all'Autorità Garante, deve essere valutata l'esigenza di procedere con la denuncia all'Autorità Giudiziaria competente, nonché con la notifica del Data Breach anche ai soggetti interessati i cui dati siano stati violati.

Nel caso in cui dal data breach possa derivare un rischio elevato per i diritti e le libertà delle persone, anche queste devono essere informate senza ingiustificato ritardo, al fine di consentire loro di prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione.

L'Ufficio Tutela Dati predispone l'eventuale comunicazione all'interessato/agli interessati, a firma del titolare, da inviarsi nei tempi e nei modi che lo stesso, anche attraverso la funzione consulenziale del DPO, individuerà come più opportuna come specificato nell'art. 34 del GDPR e tenendo conto di eventuali indicazioni fornite dall'Autorità Garante.

Per stabilire se sia necessario provvedere alla notifica agli Interessati, saranno valutati i seguenti fattori:

i. il trattamento può comportare discriminazioni, furto d'identità, perdite finanziare, disturbi psicologici, pregiudizio alla reputazione, perdita di riservatezza dei Dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo;

ii. gli Interessati rischiano di essere privati dei loro diritti, delle libertà o venga loro impedito l'esercizio del controllo sui Dati personali che li riguardano;

iii. sono trattati Dati personali che rivelano l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi a condanne penali e a reati o alle relative misure di sicurezza;

iv. 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;

v. sono trattati Dati personali di persone fisiche vulnerabili, in particolare minori;

vi. il trattamento riguarda una notevole quantità di Dati personali e un vasto numero di Interessati.

La notifica agli Interessati sarà effettuata nel caso in cui la violazione di Dati personali presenti un rischio elevato per i diritti e le libertà delle persone fisiche, a meno che non sia verificata almeno una delle seguenti condizioni:

i. sono state applicate adeguate misure tecniche e organizzative per proteggere i dati prima della violazione, in particolare quelle in grado di renderle non intelligibili per soggetti terzi non autorizzati (ad esempio, misure di cifratura);

ii. a valle della rilevazione del Data Breach, sono state adottate misure per impedire il concretizzarsi dei rischi per i diritti e le libertà degli Interessati;

iii. la notifica del Data Breach a tutti gli Interessati singolarmente comporta uno sforzo sproporzionato rispetto al rischio. In tal caso si valuterà comunque l'opportunità di procedere a una comunicazione pubblica o a una misura simile, tramite la quale gli Interessati siano comunque informati con analoga efficacia. 12) Gestione del Data Breach relativo a dati personali trattati in qualità di Responsabile del trattamento

12) Gestione del data breach in qualità di responsabile del trattamento ai sensi dell'art 28 GDPR 679/2016;

Acqua S.r.l (e le società ad essa collegate Booster srl e EMG srl) in qualità di Responsabile esterno ai trattamenti, ha l'obbligo di informare il Titolare del trattamento, senza ingiustificato ritardo, di ogni potenziale evento di data breach. Rimane salva la possibilità che sia il Responsabile stesso ad effettuare la notifica per conto del Titolare, se quest'ultimo ha rilasciato specifica autorizzazione all'interno dell'atto di nomina/contratto. Tale notifica deve essere fatta in conformità con gli articoli 33 e 34 del GDPR fermo restando la responsabilità legale in capo al Titolare del trattamento.

Qualora, a seguito di una segnalazione o nel corso dell'analisi preliminare di cui ai precedenti paragrafi, l'Ufficio Tutela Dati rilevasse che la violazione qualificabile come Data Breach riguardasse dati personali di titolarità di un soggetto terzo trattati dalla Società in qualità di Responsabile del trattamento, procede a informare –entro il termine di 24 ore dal verificarsi della violazione - il soggetto terzo titolare del trattamento.

Nel dettaglio, la comunicazione al soggetto titolare del trattamento dovrà contenere quanto meno le seguenti informazioni (oltre a quelle eventualmente richieste dallo stesso soggetto terzo titolare del trattamento):

i. Descrizione della natura della violazione dei dati personali comprensiva, ove possibile, di informazioni in merito alle categorie e al numero di Interessati nonché alle categorie e al volume approssimativo di dati personali oggetto di violazione;

ii. Nome e dati di contatto del DPO di Venis;

iii. Descrizione delle possibili conseguenze della violazione;

iv. Descrizione di eventuali misure già adottate o di cui si prevede l'adozione per porre rimedio alla violazione di dati personali e per attenuarne i possibili effetti negativi.

13) Prescrizioni per la prevenzione di data breach

Acqua S.r.l (e le società ad essa collegate Booster srl e EMG srl) ha adottato specifiche strategie volte a prevenire la verificazione di incidente alla sicurezza ai dati personali

In primo luogo, occorre che tutti i soggetti nominati quali autorizzati al Trattamento siano consapevoli dei Dati personali che trattano attraverso i propri strumenti (anche cartacei) e dispositivi a cui hanno accesso tramite i sistemi del Titolare del trattamento.

A tal fine, la presente procedura viene loro comunicata ed essi dovranno custodire tali Dati personali ed i relativi documenti con cura e in modo responsabile sia all'interno che all'esterno della propria area di lavoro.

Si precisa che i soggetti in questione sono già stati istruiti per mezzo di specifici atti di designazione e devono attenersi alle prescrizioni contenute nel Disciplinare interno contenente le norme di comportamento per l'accesso e l'utilizzo dei sistemi e delle risorse

informatiche, della navigazione Internet, della gestione della posta elettronica nonché della gestione dei documenti analogici di Acqua S.r.l. (e le società ad essa collegate Booster srl e EMG srl)

14) Schema di valutazione degli scenari

Di seguito sono illustrati alcuni esempi, non esaustivi, di possibili violazioni di dati personali, allo scopo di supportare i soggetti coinvolti nella procedura, nella valutazione in merito alla necessità di effettuare o meno la notifica di data breach all'Autorità Garante.

Tipo di data breach	**Definizione**	**Caratteristiche**
Perdita	Un insieme di dati personali, a seguito di un incidente o azione fraudolenta, non è più nella disponibilità del Titolare, ma potrebbe essere nella disponibilità di terzi (in maniera lecita o illecita). In caso di richiesta del dato da parte dell'interessato non è possibile produrlo, mentre è possibile che terzi ne possano avere impropriamente accesso	Dati non recuperabili o provenienti procedure/processi non ripetibili e che non possono, quindi, essere ulteriormente generati Dati la cui indisponibilità lede i diritti fondamentali dell'interessato Dati per i quali la divulgazione, conseguente alla perdita, possa ledere i diritti fondamentali dell'interessato
Modifica	Un insieme di dati personali, a seguito di un incidente o azione fraudolenta, è stato irreversibilmente modificato, senza la possibilità di ripristinare lo stato originale. In caso di richiesta del dato da parte dell'interessato non è possibile produrlo con	Dati non per i quali non è possibile avere certezze sulla consistenza e sull'assenza di alterazioni

	la certezza che non sia stato alterato	
Divulgazione non autorizzato ai dati	Un insieme di dati personali (e riconducibili all'individuo in maniera diretta o indiretta), a seguito di un incidente o azione fraudolenta, è stato trasmesso a terze parti senza il consenso dell'interessato o in violazione del regolamento dell'organizzazione	Dati per i quali la divulgazione, conseguente alla perdita, possa ledere i diritti fondamentali dell'interessato
Accesso non autorizzato	Un insieme di dati personali (e riconducibili all'individuo in maniera diretta o indiretta), sono stati resi disponibili per un intervallo di tempo a persone non titolate ad accedere al dato secondo principio di pertinenza o eccedenza, oppure secondo i regolamenti dell'organizzazione	Dati per i quali la divulgazione, conseguente alla perdita, possa ledere i diritti fondamentali dell'interessato
Indisponibilità temporanea	Un insieme di dati personali, a seguito di un incidente o azione fraudolenta o involontaria, non è più disponibile per un periodo di tempo che lede	Dati per i quali l'indisponibilità eccede il massimo consentito dai regolamenti dell'organizzazione e possa ledere i diritti fondamentali dell'interessato

	i diritti dell'interessato	

Un data breach, quindi, non è solo un attacco informatico, ma può consistere anche in un accesso abusivo, un incidente (es. un incendio o una calamità naturale), oppure nella semplice perdita/furto di un dispositivo mobile di archiviazione (es. chiavetta USB, disco esterno), di un pc portatile, di un tablet/smartphone, tale da permettere la sottrazione di documenti dati personali.

I casi di data breach per quanto descritto si estendono anche ai documenti cartacei o su supporti analogici.

La comunicazione involontaria di documenti non contenenti alcun dato personale non è considerata un data breach ma un errore procedurale