REGOLAMENTO RELATIVO ALLA VIOLAZIONE DEI DATI PERSONALI – DATA BREACH

Art. 1 - Definizione di Data Breach (Reg. UE 679/2016 art. 4 c. 1 punto 12)

Si intende per «violazione dei dati personali» "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". Tali violazioni possono riguardare sia trattamenti informatici che qualunque altra attività non di tipo informatico che comporti trattamento di dati (es. trattamenti su documenti cartacei, trattamento di immagini, comportamenti umani ecc).

Art. 2 - Notifica all'Autorità di controllo (Reg 2016/679 art. 33)

Quando la violazione dei dati personali presenta un rischio per i diritti e le libertà delle persone fisiche il Titolare del trattamento, nella persona del rappresentante legale o di suo delegato, ne fa notifica all'Autorità di controllo.

La notifica deve avere i contenuti stabiliti all'art. 33 c.2 e deve avvenire, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui il titolare ne è venuto a conoscenza. Le 72 decorrono dalla data e ora della comunicazione al Titolare (rappresentato dalla Direzione Strategica) e/o al DPO da parte del Delegato al trattamento, interno all'azienda, se l'eventuale "data breach" è rilevato in azienda, nelle modalità indicate all'art. 4. Qualora il data breach sia riscontrato dal reclamo o dalla segnalazione di un utente/paziente, i tempi di notifica decorrono dalla data di protocollazione e assegnazione del reclamo. Qualora la notifica all'Autorità di controllo non sia effettuata entro le 72 ore, occorre motivare il ritardo. La notifica non è dovuta se il Titolare ritiene improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, nell'ambito delle valutazioni istruttorie che emergono dal gruppo di lavoro di cui all'art. 4.

Art 3 - Comunicazione agli interessati (Reg 2016/679 art. 34)

Quando la violazione dei dati personali presenta un rischio **elevato** per i diritti e le libertà delle persone fisiche e non ci sono le condizioni di cui all'art. 34 c. 3 lett. a) b) e c), il Delegato al trattamento dei dati ne dà comunicazione agli interessati (intendendo per tali anche i controinteressati, che potrebbero essere per esempio, in caso di reclamo, soggetti diversi da chi presente il reclamo su cui il "data breach" può produrre effetti). Qualora il "data breach" coinvolga più interessati, il cui trattamento dei dati rientra negli ambiti di competenza di più Delegati, la comunicazione è effettuata direttamente dal Titolare, nella persona del Direttore Generale. La comunicazione agli interessati avrà i seguenti contenuti minimi:

- Descrizione della violazione
- Misure vigenti al momento della violazione
- Misure adottate nell'immediato per attenuare l'impatto sui diritti degli interessati
- Eventuali suggerimenti agli stessi interessati per contenere gli effetti negativi del data breach

Art. 4 – Ruoli aziendali e "gruppo di valutazione" del data berach

Quando l'episodio, riconducibile alla fattispecie descritta all'art. 1, è rilevato all'interno della ASST, chiunque ne abbia notizia o conoscenza, ha l'obbligo di segnalarlo tempestivamente al proprio Direttore di SC, o Responsabile di SSD o Responsabile di funzioni/SS di staff, quali "delegati" al trattamento dei dati da l Direttore generale.

I soggetti di cui sopra per le funzioni di raccordo con il Titolare, ai fini di una corretta gestione del processo, dovranno comunicare al Titolare (come individuato all'art. 2) e/o al DPO l'accaduto, previa verifica della fondatezza della segnalazione, i cui contenuti minimi sono quelli indicati all' Allegato 1, anche mediante l'uso di mail.

L'obbligo di comunicare tempestivamente eventuali violazioni di dati personali ricade anche sul Responsabile del trattamento nominato ai sensi dell'art. 28 del Reg UE 2016/679, come previsto nel modello di nomina adottato in azienda.

Il Titolare, o il DPO a supporto del Titolare, coinvolge i Delegati competenti, per raccogliere tutte le informazioni utili alle valutazioni necessarie, mediante mail. Tali soggetti fanno parte del "Gruppo di valutazione" deputato alla disanima dell'accaduto, ciascuno per la propria parte, per arrivare ad una valutazione congiunta dell'esistenza delle condizioni per la notifica all'Autorità di controllo e/o la comunicazione agli interessati di cui agli articoli precedenti.

Per la dinamicità degli eventi e per la ristrettezza dei tempi posti dalla legge, le consultazioni, la raccolta e lo scambio di informazioni atte a maturare le decisioni da prendere, avvengono anche in modo dinamico (mediante mail) e non si esauriscono necessariamente in un momento unico di incontro tra tutti i soggetti parte del "Gruppo di valutazione".

Tale gruppo è composto dal Titolare (rappresentato da uno o più Direttori della Direzione strategica), dal DPO, da un rappresentante del SIA (se la violazione riguarda l'uso degli strumenti ICT), dal/i Delegato/i al trattamento dei dati coinvolti negli accadimenti.

Di volta in volta è chiamato a dare il proprio contributo anche il Responsabile del trattamento ex art 28 (o un suo delegato), se coinvolto nelle attività di trattamento a cui il "data breach" si riferisce.

Il gruppo è integrato dalla presenza del Responsabile della comunicazione nel caso in cui si debba valutare una comunicazione agli interessati, su larga scala, con mezzi di stampa o di divulgazione mediatica.

Per le valutazioni più complesse, per le quali è necessario interagire anche con soggetti esterni, quali ARIA s.p.a, potrà essere messa a punto una più specifica "istruzione operativa".

Art. 5 - Criteri di valutazione

5.1 Il data breach può riassumersi nelle seguenti tipologie:

- violazione della riservatezza e cioè disvelamento o accesso indebito o accidentale ai dati.
- violazione della disponibilità dei dati e cioè indebito o accidentale impedimento (*anche temporaneo)* all'accesso dei dati o distruzione dei dati.
- violazione della integrità dei dati e cioè indebita o accidentale alterazione dei dati.

5.2 In particolare quando trattasi di violazione dei dati mediante "violazione delle banche dati elettroniche (lettura, copia, alterazione, cancellazione, furto)" che comporti:

1. un rischio per i diritti e le libertà delle persone fisiche;
2. un rischio elevato per i diritti e le libertà delle persone fisiche;

il gruppo di valutazione si avvale del modello elaborato da ENISA (working document, v1.0, december 2013) che rileva il livello di violazione in base a 3 criteri (Tipologia di dati, Facilità

di identificazione del soggetto, Circostanze di violazione) mediante la risposta a domande funzionali a determinare il livello di impatto.
Il modello, il cui schema è contenuto nell' Allegato 2 al presente Regolamento e parte integrante dello stesso, rielabora una valutazione atta a definire il livello di rischio per la notifica all'Autorità di controllo e per la comunicazione agli interessati.

5.3 Il gruppo di valutazione può fare ulteriori e differenti valutazioni anche per le ipotesi di violazione non valutabili secondo il modello di cui sopra, tenendo conto dei seguenti parametri indicati al considerando 85 del Reg. UE 2016/679:

- limitazione dei diritti delle persone fisiche
- perdita del controllo dei propri dati personali
- discriminazioni
- furto o usurpazione di identità
- perdite finanziarie
- decifratura non autorizzata della pseudonimizzazione
- pregiudizio alla reputazione
- perdita di riservatezza dei dati protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo per la persona interessata.

Art. 6 - Registro delle violazione art 33 c.5

Il Titolare, mediante la redazione di un Registro, detenuto nella cartella d'ufficio delle attività "privacy", con i contenuti indicati all' Allegato 3, documenta qualsiasi violazione di dati personali, comprese le violazioni che non comportano un rischio, o un rischio elevato, per i diritti e le libertà delle persone fisiche, tali da richiedere la notifica all'Autorità di controllo e/o la comunicazione agli interessati.

Art 7 - Clausole finali

Per tutto quanto non specificato nel presente regolamento vale quanto definito negli artt. 33 e 34 del Reg. UE 2016/679.

Allegato 1

INDICAZIONE DEI CONTENUTI MINIMI DELLA SEGALAZIONE PER VIOLAZIONE DEI DATI PERSONALI (DATA BREACH) AD USO DEI DELEGATI AL TRATTAMENTO

1) DESCRIZONE DELL'EVENTO E NATURA DELLA VIOLAZIONE

2) CATEGORIE E NUMERO (anche indicativo se non definito) DEGLI INTERESSATI

3) POSSIBILI CONSEGUENZE DELLA VIOLAZIONE

4) MISURE IN ATTO AL MOMENTO DELLA VIOLAZIONE E MISURE DI CUI SI PROPONE L'ADOZIONE PER PORRE RIMEDIO ALLA VIOLAZIONE

Data e firma del Delegato al trattamento

Allegato2

VALUTAZIONE DATA BREACH

per i casi di violazione delle banche dati elettroniche (lettura, copia, alterazione, cancellazione, furto)

Modello elaborato da ENISA

Step 1 - Tipologia di dati

1.1) Indicare la tipologia di dati e scegliere tra le opzioni proposte:

DATI	OPZIONI	Valore
COMUNI	La violazione riguarda "dati comuni" e il Titolare non è a conoscenza di alcun fattore aggravante.	1
	Il volume di "dati comuni" e/o le caratteristiche del Titolare sono tali da consentire una certa profilazione dell'individuo.	2
	I "dati comuni" e/o le caratteristiche del Titolare possono portare a supposizioni sullo stato di salute dell'individuo, sulle preferenze sessuali, sulle convinzioni politiche o religiose.	3
	Quando a causa di determinate caratteristiche dell'individuo (ad esempio, gruppi vulnerabili, minori), le informazioni possono essere fondamentali per la loro sicurezza personale o condizioni fisiche/psicologiche.	4
COMPORTAMENTALI	La natura dei dati non fornisce alcuna comprensione sostanziale delle informazioni comportamentali dell'individuo o i dati possono essere raccolti facilmente attraverso fonti disponibili pubblicamente (ad esempio tramite ricerche web).	1
	La violazione coinvolge "dati comportamentali" e il Titolare non è a conoscenza di fattori aggravanti o di diminuzione.	2
	Il volume di "dati comportamentali" e/o le caratteristiche del Titolare sono tali da consentire la creazione di un profilo	3

	dell'individuo, esponendo informazioni dettagliate sulla sua vita quotidiana e sulle sue abitudini.	
	Se è possibile creare un profilo basato sui dati sensibili di una persona.	4
FINANZIARI	La natura dei dati non fornisce alcuna comprensione sostanziale delle informazioni finanziarie dell'individuo (ad esempio il fatto che una persona sia il cliente di una determinata banca senza ulteriori dettagli).	1
	I dati includono informazioni finanziarie, ma non fornisce ancora informazioni significative sullo stato/situazione finanziaria dell'individuo (ad esempio numeri di conti bancari semplici senza ulteriori dettagli).	2
	La violazione coinvolge "dati finanziari" e il Titolare del trattamento non è a conoscenza di fattori aggravanti o di diminuzione.	3
	Quando a causa della natura e/o del volume dell'insieme di dati specifico, vengono divulgate informazioni complete sul piano finanziario (ad esempio, carta di credito)	4
PARTICOLARI	La natura dei dati non fornisce alcuna comprensione sostanziale delle informazioni specifiche dell'individuo o i dati possono essere raccolti facilmente attraverso fonti disponibili pubblicamente (ad esempio tramite ricerche web).	1
	La natura dei dati può portare a ipotesi generali.	2
	La natura dei dati può portare a supposizioni su informazioni sensibili e riguardanti lo stato di salute.	3
	La violazione riguarda "dati particolari", incluso lo stato di salute, e il Titolare non è a conoscenza di alcun fattore di diminuzione.	4

Step 2 - Facilità identificazione soggetto

DATO	OPZIONI	Valore
Nome completo È considerato come l'identificatore diretto più comune, ma il punteggio può variare a seconda del caso, poiché il nome completo non è sempre di per sé univoco dell'individuo. Ad esempio, quando l'identificazione viene eseguita utilizzando solo il nome completo dell'individuo:	in tutta la popolazione di una zona in cui molte persone condividono lo stesso nome completo	0,25 (Trascurabile)
	nella popolazione di una zona in cui poche persone condividono lo stesso nome completo.	0,5 (limitato)
	in tutta la popolazione di una zona in cui poche o nessuna persona condivide lo stesso nome completo.	0,75 (Significativo)
	nella popolazione di una zona utilizzando anche data di nascita e indirizzo e-mail	1 (massimo)
Documento di riconoscimento Sono considerati come identificatori univoci e possono essere utilizzati per individuare l'individuo, purché sia possibile collegarli a un database di riferimento (ad esempio collegando una carta d'identità a una determinata persona). Ad esempio, quando l'identificazione viene eseguita utilizzando solo uno di questi numeri	quando non sono fornite altre informazioni sull'individuo o non è possibile trovare ulteriori informazioni a meno che non si ottenga l'accesso al database di riferimento	0,25 (Trascurabile)
	quando l'identificativo rivela ulteriori informazioni identificative sull'individuo (ad es. Numero di previdenza sociale che rivela la data di nascita) ed è collegato ad altri dati (ad esempio indirizzo postale o email).	0,75 (Significativo)
	quando sono disponibili anche le informazioni dal database di riferimento (ad esempio carta d'identità e nome completo e/o immagine).	1 (massimo)
Telefono o indirizzo Sono entrambi identificatori indiretti, che possono anche essere usati per comunicare o accedere all'individuo, quando	in tutta la popolazione di una zona quando il numero / indirizzo non è registrato in un registro disponibile al pubblico.	0,25 (Trascurabile)
	in tutta la popolazione di una zona e il numero / indirizzo non è registrato in un registro disponibile pubblicamente	0,5 (limitato)

l'identificazione si basa solo su uno di questi due identificatori:	(identificazione possibile attraverso la comunicazione).	
	nella popolazione di una zona e il numero / indirizzo è incluso nel registro disponibile pubblicamente.	1 (massimo)
Email È un identificatore indiretto, che può essere utilizzato per comunicare con l'individuo e in alcuni casi può includere informazioni sul suo nome (nome e/o cognome) .Quando l'identificazione si basa sulla posta elettronica:	quando l'indirizzo e-mail non rivela altre informazioni di identificazione (ad es. Nome) e non è utilizzato come indirizzo primario dell'individuo in siti internet, forum o social network.	0,25 (Trascurabile)
	quando l'indirizzo di posta elettronica non rivela altre informazioni di identificazione (ad es. Nome) ma è utilizzato come indirizzo primario dell'individuo in siti internet, forum o social network (ricercabili sul web).	0,75 (Significativo)
	quando l'indirizzo email rivela il nome dell'individuo e viene utilizzato come indirizzo principale in siti internet, forum o social network (ricercabili sul Web	1 (Massimo)).
Fotografia Potrebbe essere un identificatore diretto o indiretto, a seconda dei casi, ad esempio quando l'identificazione si basa solo su un'immagine:	quando l'immagine non è chiara o vaga (ad esempio, videosorveglianza da una lunga distanza).	0,25 (Trascurabile)
	quando l'immagine non è chiara ma include informazioni aggiuntive che potrebbero portare all'identificazione dell'individuo.	05 (Limitato)
	quando l'immagine è chiara ma nessun'altra informazione di identificazione è collegata ad essa.	0,75 (Significativo)
	quando l'immagine è chiara e collegata ad alcune informazioni aggiuntive (ad esempio informazioni sull'appartenenza a un gruppo specifico, indirizzo di casa, ecc.).	1 (Massimo)
Codice identificativo/Alias/Iniziali La codifica si riferisce all'assegnazione di un numero identificativo univoco a ciascun individuo, ad es. nel contesto di un database specifico. L'uso di alias è una forma di pseudonimizzazione, nel senso che un identificatore specifico (di	quando il codice/alias non rivela e non può essere collegato a nessun altro dato personale sulla persona a meno che non si abbia accesso al database di riferimento.	0,25 (Trascurabile)
	quando l'alias rivela alcuni dati sull'individuo (ad esempio, il nome) ed è collegato ad altri dati personali (ad esempio l'indirizzo email dell'individuo).	0,75 (Significativo)

solito il nome completo dell'individuo) è sostituito da un alias (pseudonimo). Le iniziali sono un tipo di alias estratto dal nome completo dell'individuo. Come nel caso degli identificatori univoci, i codici e gli alias possono essere utilizzati per identificare l'individuo fintanto che è possibile collegarli a un database di riferimento (ad esempio collegando il codice/alias al nome completo di una particolare persona) Quando l'identificazione è basato sulla codifica o l'uso di alias:		
	quando l'alias rivela il nome completo dell'individuo oi dati dal database di riferimento sono anche disponibili.	1 (Massimo)

Step 3 - Circostanze di violazione

TIPOLOGIA DI VIOLAZIONE	OPZIONI	Valore
Perdita di riservatezza	I dati sono esposti a rischi di riservatezza senza prove dell'esistenza di un trattamento illecito. Ad esempio un file cartaceo o un laptop viene perso durante il trasporto o l'apparecchiatura viene smaltita senza distruzione dei dati personali.	0
	I dati sono disponibili ad un numero noto di destinatari. Ad esempio viene inviata un e-mail con dati personali, ad un certo numero di destinatari. Cosi alcuni utenti potrebbero accedere agli account di altri clienti.	0,25
	I dati disponibili ad un numero sconosciuto di destinatari. Ad esempio dati pubblicati su internet; oppure un dipendente vende un CD con i dati dei clienti; oppure un sito Web è configurato in modo errato e rende accessibili pubblicamente i dati.	0.5
Perdita di integrità	I dati sono modificati ma senza alcun uso identificato errato o illegale. Ad esempio i registri di un database con dati personali sono stati erroneamente aggiornati ma l'originale è stato ottenuto prima che si verificasse l'uso dei dati modificati.	0
	I dati sono modificati ed eventualmente utilizzati in modo errato o illegale ma con possibilità di recupero.	0,25

	Ad esempio è stato modificato un dato necessario per un servizio online e l'individuo deve richiedere il servizio in modalità offline.	
	Esempi di dati modificati ed eventualmente usati in modo errato o illegale senza possibilità di recupero. (ad esempio gli esempi precedenti + l'originale non possono essere recuperati).	0.5
Perdita di disponibilità	I dati possono essere recuperati senza difficoltà. Ad esempio una copia del file viene persa ma sono disponibili altre copie, un database è danneggiato ma può essere facilmente ricostruito da altri database.	0
	Esempi di indisponibilità temporale, ad esempio un database è danneggiato ma può essere ricostruito da altri database, sebbene sia richiesta qualche elaborazione l'informazione può essere fornita di nuovo dall'individuo.	0,25
	Esempi di indisponibilità totale (i dati non possono essere recuperati dal Titolare) ad esempio, un file viene perso / database danneggiato, non c'è il backup di questa informazione e non può essere fornito dall'individuo.	0,5
Attacco interno o esterno	La violazione mira a causare problemi al Titolare e/o danneggiare le persone. Ad esempio, il Titolare è stato vittima di un attacco cyber da esterno o da un dipendente che ad esempio ha condiviso dati critici degli interessati per danneggiarli.	0,5

Step 4 - Indicare il numero di interessati coinvolti nella violazione

NUMERO	Valore
0-10	0,6
10-100	0,7
100-1000	1
Maggiore di 1000	1,1

Step 5 - Indicare se i dati coinvolti nella violazione sono protetti da misure che non li rendono intelligibili

MISURE DI PROTEZIONE	Valore
cifratura	- 1,5

pseudoanonimizzazione	- 1
no	0

LIVELLO DI RISCHIO RISULTANTE

Sarà calcolato il valore di rischio del data breach che potrà risultare:

Range di valori	Livelli di rischio	Descrizione
<2	**Trascurabile**	Gli individui non sarebbero interessati o potrebbero incontrare alcuni inconvenienti, che supererebbero senza alcun problema (ad esempio tempo trascorso a reinserire informazioni, ecc.)
2 ≤ SE < 3	**Basso**	Gli individui potrebbero incontrare alcuni disagi, che sarebbero in grado di superare con difficoltà limitate (ad esempio ritardo di accesso ai servizi aziendali, stress, ecc.)
3 ≤ SE< 4	**Medio**	Gli individui potrebbero incontrare conseguenze che dovrebbero essere in grado di superare anche con alcune difficoltà (ad esempio appropriazione indebita di fondi, danni alla proprietà, citazione in giudizio, peggioramento della salute, ecc.)
4 ≤ SE	**Alto**	Gli individui potrebbero incontrare conseguenze significative, o addirittura irreversibili, che non possono superare (ad esempio difficoltà finanziarie come debito sostanziale o incapacità lavorativa, disturbi psicologici o fisici a lungo termine, ecc.)

NOTIFICA AL GARANTE	Sì
	NO
	DA VALUTARE
COMUNICAZIONE AGLI INTERESSATI	Sì
	NO
	DA VALUTARE

Allegato 3

SCHEMA REGISTRO DELLE VIOLAZIONI

PROGRESSIVO	SEGNALAZIONE PERVENUTA CON MAIL (DATA E ORA)	SEGNALATORE *(interno o esterno all'ASST)*	BREVE DESCRIZIONE DELLA VIOLAZIONE E POSSIBILI CONSEGUENZE	TIPOLOGIA DEI DATI *Indicare se: personali attinenti alla salute genetici giudiziari biometrici*	INTERESSATI O CATEGORIE DI INTERESSATI	MISURE IN ESSERE AL MOMENTO DELLA VIOLAZIONE/INCIDENTE *indicare se cifratura o pseudomizzazione per dati informatici o strategie di protezione per dati cartacei*	MISURE ADOTTATE PER PORRE RIMEDIO ALLA VIOLAZIONE/INCIDENTE	***AZIONI DI MILIORAMENTO***	NOTIFICA AL GARANTE *Se sì, data e ora invio. Se no, breve descrizione della motivazione*	COMUNICAZIONE AGLI INTERESSATI *Se sì, data e mezzo invio Se no breve descrizione della motivazione*