REGOLAMENTO DATA BREACH

Sommario

REGOLAMENTO DATA BREACH

Art. 1 Premessa

I dati personali conservati, trasmessi o trattati da aziende e pubbliche amministrazioni possono essere soggetti al rischio di perdita, distruzione o diffusione indebita, ad esempio a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi, come incendi o altre calamità; queste violazioni di dati personali (di seguito *data breach*) possono comportare pericoli significativi per la privacy degli interessati ai quali si riferiscono i dati violati.

Il *data breach* può interessare sia documenti cartacei che documenti conservati su supporti analogici e può consistere non solo in un attacco informatico, ma anche in un accesso abusivo a un edificio in cui siano custoditi dati personali o a un sistema informatico, in un incidente (es. un incendio o una calamità naturale), nella semplice perdita accidentale di un dispositivo mobile di archiviazione (es. chiavetta USB, disco esterno) o nella sottrazione di documenti con dati personali (es. furto di un notebook di un dipendente o di un fascicolo cartaceo).

Un tanto premesso, il GDPR dispone che in caso di *data breach* il Titolare del trattamento notifichi la violazione all'Autorità di controllo competente ai sensi dell'articolo 55 senza ingiustificato ritardo e, se 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 non sia effettuata entro 72 ore, la notifica all'Autorità di controllo è corredata di una giustificazione motivata.

Il presente documento, indirizzato a tutti i dipendenti di Friuli Venezia Giulia Strade S.p.A. (di seguito FVGS) e a tutti i Responsabili esterni del trattamento dei dati, ha l'obiettivo di indicare le opportune modalità di gestione del *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 – GDPR** in relazione alle modalità di segnalazione dell'evento al Titolare del trattamento e al Garante della privacy, alla valutazione dell'evento stesso e all'eventuale comunicazione del medesimo agli interessati.

Art. 2 Fonti e riferimenti normativi

- **D.Lgs. n.196/03 – Codice della privacy** (come modificato dal Decreto di adeguamento della normativa nazionale ai principi del GDPR - D.Lgs n.101/18);
- **Regolamento Generale sulla Protezione dei dati UE (GDPR) n.679/2016;**
- **Delibera della Giunta Regionale n.377/2017** - Progetto di **Assessment di FVGS** redatto da INSIEL S.p.A. – Autorizzazione all'integrazione del Sistema Informativo di Friuli Venezia Giulia Strade nel Sistema Informativo regionale;
- **D.Lgs. n.101/2018 - Decreto di adeguamento** della normativa nazionale ai principi del Regolamento Europeo relativo alla protezione delle persone fisiche riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE Regolamento generale sulla protezione dei dati;
- **Delibera della Giunta Regionale n.1109/2019 – DLGS 285/1992 e successive modifiche e integrazioni** (Nuovo Codice della Strada). LR 9/2011, **Assessment di FVGS** implementazione;
- **Delibera della Giunta Regionale n.1985/2021 – Aggiornamento dell'indirizzo di cui alla DGR 377/2017. Piano informatico FVGS**: Autorizzazione alla Convenzione diretta tra FVGS e Insiel.

Art. 3 Definizioni da GDPR

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, punto 1).

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, punto 2).

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, punto 6).

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 (art. 4, punto 7) cioè FVGS.

Responsabile esterno del trattamento dei dati: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento.

***Data Protection Officer (DPO)*:** la persona fisica individuata come Responsabile della protezione dei dati personali ai sensi del GDPR (in particolare artt. 37, 38, 39).

Autorizzato al trattamento: la persona fisica, espressamente designata, che opera sotto l'autorità del Titolare del trattamento, con specifici compiti e funzioni connessi al trattamento dei dati personali (art. 4, punto 10).

Autorità di controllo: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51; in Italia è tuttora il Garante della Privacy;

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, punto 12).

Art. 4 Gestione *data breach* interno

Ogni dipendente autorizzato a trattare dati, qualora venga a conoscenza di un potenziale caso di *data breach*, avvisa **entro e non oltre 48 ore**, il DPO interno tramite il modello M 14.02 *Data breach* - comunicazione interna; la comunicazione deve contenere una descrizione più precisa possibile per permettere un'agevole valutazione dell'evento e della necessità o meno di segnalarlo al Garante della privacy.

Il DPO effettua una valutazione dell'evento avvalendosi anche delle competenze dell'UO Sistemi informatici e telecomunicazioni (di seguito CED), utilizzando la tabella riportata all'Art. 8 Valutazione di data breach, contenente alcuni esempi di *data breach*.

Sulla scorta delle determinazioni raggiunte, il DPO predispone l'eventuale comunicazione al Garante della privacy (M 14.04 *Data breach* - comunicazione a Garante), a firma del Titolare del trattamento, da inviare senza ingiustificato ritardo e, se possibile, entro 72 ore a decorrere dal momento in cui il Titolare è venuto a conoscenza dell'evento; oltre il termine delle 72 ore, la notifica deve essere corredata dalle motivazioni del ritardo.

Ai sensi dell'art. 33, par. 3, GDPR la comunicazione deve come minimo:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del DPO presso cui ottenere più informazioni;
c) descrivere le probabili/possibili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi.

Art. 5 Gestione *data breach* esterno

Ogniqualvolta la FVGS/Titolare del trattamento debba affidare il trattamento di dati ad un soggetto terzo/Responsabile del trattamento c.d. esterno, è tenuta a stipulare con tale soggetto uno specifico contratto che lo vincoli al rispetto delle istruzioni impartitegli dal Titolare in materia di protezione dati: pertanto è necessario che la presente procedura di segnalazione di *data breach* sia inclusa nel suddetto contratto al fine di obbligare il Responsabile ad informare il Titolare del trattamento di ogni potenziale evento di violazione di dati personali senza ingiustificato ritardo.

Ad ogni Responsabile del trattamento viene comunicato il contatto del DPO affinché entro e non oltre 48 ore dal momento in cui è venuto a conoscenza di un potenziale *data breach* che riguardi dati di cui l'azienda sia Titolare, lo informi tramite mail.

Il DPO effettua una valutazione dell'evento avvalendosi anche delle competenze del CED, utilizzando la tabella riportata all'Art. 8 Valutazione di data breach, contenente alcuni esempi di *data breach*.

Sulla scorta delle determinazioni raggiunte, il DPO predispone l'eventuale comunicazione al Garante della privacy (M 14.04 *Data breach* - comunicazione a Garante), a firma del Titolare del trattamento, da inviare senza ingiustificato ritardo e, se possibile, entro 72 ore a decorrere dal momento in cui il Titolare è venuto a conoscenza dell'evento; oltre il termine delle 72 ore, la notifica deve essere corredata dalle motivazioni del ritardo.

Il contenuto della comunicazione è lo stesso di quello della comunicazione in caso di *data breach* interno (v. Art. 4) e disponibile sul modulo M 14.03 *Data breach* - comunicazione esterna).

Art. 6 Modalità di comunicazione agli interessati

Quando la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento deve comunicare la violazione all'interessato/agli interessati senza ingiustificato ritardo, descrivendo con linguaggio semplice e chiaro la natura della violazione dei dati personali e trasmettendo altresì le informazioni di cui alle lett. b, c e d dell'art. 33 GDPR (v. Art. 4).

Il DPO predispone quindi la comunicazione all'interessato/agli interessati compilando il modulo M 14.05 (*Data breach* – comunicazione a interessato), a firma del Titolare del trattamento, da inviarsi tempestivamente e tenendo conto di eventuali indicazioni fornite dall'Autorità di controllo.

La comunicazione all'interessato non è richiesta se ricorre almeno una delle seguenti condizioni:

a) il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b) il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

c) detta comunicazione richiederebbe sforzi sproporzionati. In tale caso, allo scopo di informare tutti gli interessati si procede alla pubblicazione sul sito internet aziendale di un avviso.

Di seguito si riportano altresì alcuni criteri a disposizione del DPO per la valutazione del rischio in relazione alla scelta sulla comunicazione o meno della violazione al Garante della Privacy e/o all'interessato/agli interessati:

- Controlli e misure di sicurezza già adottate: se la violazione non è suscettibile di causare danni agli interessati la comunicazione non è necessaria;
- Controlli e misure di sicurezza adottate subito dopo la violazione: se si è impedito che la violazione causi danni agli interessati la comunicazione non è necessaria;
- Quantità di dati personali oggetto della violazione: in caso di dati personali relativi a molti interessati la comunicazione è sempre opportuna, eventualmente con misure che permettano l'avviso di molte persone contemporaneamente (per es. notizia pubblicata sul sito internet aziendale);
- Tipologia dei dati personali oggetto della violazione: in caso di dati sensibili/relativi a condanne penali o a reati, di credenziali di autenticazione o di dati relativi al traffico telefonico/telematico la comunicazione va sempre effettuata;
- Attualità dei dati personali oggetto della violazione: in caso di dati risalenti, ovvero raccolti molto tempo prima, la comunicazione potrebbe non essere necessaria per la minore probabilità che ciò comporti danni per gli interessati;
- Identificabilità degli interessati a cui si riferiscono i dati personali coinvolti dalla violazione: se i dati sono stati correttamente anonimizzati non è necessario effettuare la comunicazione;
- Gravità delle conseguenze dovute alla violazione: qualora i dati possano comportare furto o usurpazione di identità, danni economici, danni fisici, umiliazioni gravi o danno alla reputazione degli interessati la comunicazione è sempre opportuna;
- Contesto specifico in cui la violazione si è verificata: in alcuni ambiti lavorativi vanno utilizzate una maggiore delicatezza e sensibilità (per es. quello sanitario) rispetto ad altri, pertanto la valutazione della necessarietà della comunicazione ne deve tenere conto.

Art. 7 Registro delle violazioni

Il DPO compila e cura l'aggiornamento del Registro delle violazioni di dati personali (M 14.01 Registro *data breach*), inserendovi anche la descrizione degli eventi non comunicati al Garante.

In esso sono descritte le circostanze in cui la violazione dei dati si è verificata, le sue conseguenze e i provvedimenti adottati per porvi rimedio affinché il Garante della privacy possa verificare il rispetto delle disposizioni contenute nell'art. 33 del GDPR. Qualora e nella misura in cui non sia possibile fornire contestualmente le informazioni, le stesse possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

La scelta e le motivazioni che hanno portato a non notificare l'evento sono tempestivamente riportate nel registro delle violazioni a cura del DPO.

Art. 8 Valutazione di *data breach*

La tabella sottoriportata contiene un elenco, non esaustivo, di possibili violazioni di dati personali, allo scopo di supportare tutti i soggetti coinvolti nella procedura nella corretta valutazione della necessità di effettuare o meno la notifica all'Autorità Garante.

Tipo di *data breach*	Definizione	Esempi
Distruzione	Un insieme di dati personali, a seguito di un incidente o di un'azione fraudolenta, non è più nella disponibilità né del Titolare né di altri; in caso di richiesta del dato da parte dell'interessato, pertanto, non sarebbe possibile produrlo	Incendio di archivio cartaceo; Distruzione accidentale o dolosa di un documento originale cartaceo privo di copia; Cancellazione accidentale o dolosa di dati personali non recuperabili nemmeno tramite *backup;* Incendio/allagamento a sistemi presenti nel CED.
Perdita	Un insieme di dati personali, a seguito di un incidente o di un'azione fraudolenta, non è più nella disponibilità del Titolare, ma potrebbe essere nella disponibilità di terzi (lecitamente o illecitamente); in caso di richiesta del dato da parte dell'interessato, pertanto, non sarebbe possibile produrlo; sarebbe, inoltre, possibile che terzi abbiano impropriamente accesso al dato	Smarrimento/furto di un documento/fascicolo originale cartaceo privo di copia; Smarrimento/furto di un supporto di memoria (per es. chiavetta usb) contenente dati originali in unica copia (qualora i dati personali non siano crittografati per renderli inintelligibili); Smarrimento/furto PC portatile/ *smartphone.*
Modifica	Un insieme di dati personali, a seguito di un incidente o di un'azione fraudolenta, è stato irreversibilmente modificato senza possibilità di ripristinare lo stato originale; pertanto, in caso di richiesta del dato da parte dell'interessato, non sarebbe possibile produrlo con la certezza che si tratti della versione originale.	Guasto o attacco informatico che altera dati personali non recuperabili nemmeno tramite *backup.*
Divulgazione non autorizzata	Un insieme di dati personali riconducibili direttamente o indirettamente a un individuo, a seguito di un incidente o di un'azione fraudolenta, viene trasmesso a terze parti senza il consenso dell'interessato o in violazione della normativa applicabile.	Spedizione accidentale o dolosa di una lettera contenente dati personali (appartenenti a categorie particolari e non) alla persona sbagliata o senza l'autorizzazione del superiore competente; Divulgazione di dati ottenuti tramite un accesso informatico al sistema informatico aziendale.
Accesso non autorizzato	Un insieme di dati personali, riconducibili direttamente o indirettamente a un individuo, è stato reso disponibili per un certo lasso di tempo a persone non legittimate all'accesso a detti dati ai sensi della normativa applicabile e il Regolamento della Società.	Accesso a dati personali (sensibili e non) di altri interessati a causa di un attacco informatico o di un malfunzionamento del sistema informatico aziendale; Accesso fraudolento ad archivio cartaceo/informatico.
Indisponibilità temporanea del dato	Un insieme di dati personali, a seguito di incidente, azione fraudolenta o involontaria, non è disponibile per un certo lasso di tempo ledendo i diritti dell'interessato.	Sito internet *offline* per motivi che non dipendono dalla Società (*black out* elettrico – problemi di connessione).