POLITICA PER LA GESTIONE DEL DATA BREACH

INDICE

1. STATO DEL DOCUMENTO

Di seguito viene riportata una tabella dove è indicato lo stato del documento con indicazione della prima emissione e delle varie revisioni del documento stesso.

N. revisione	Data documento	Motivo
00	30/07/2019	Emissione del documento
01	28/01/2020	Aggiornamento Allegato A

2. GENERALITÀ

Il presente documento descrive il processo adottato per la gestione delle violazioni di sicurezza che comportano gravi rischi dei diritti e delle libertà degli Interessati, le cui informazioni personali sono trattate e custodite presso i sistemi IT e presso i locali del Titolare del trattamento.
Il *Data Breach* è una violazione della sicurezza, che comporta accidentalmente o in modo illecito la distruzione, perdita, modifica, divulgazione, accesso, copia o consultazione non autorizzate di dati personali trasmessi, conservati o comunque trattati. Ciò può avvenire a seguito di un attacco informatico, di un accesso abusivo, di un incidente (es. incendio, allagamento, etc.) o per la perdita di un supporto informatico (smartphone, notebook, chiavetta USB, etc.) o per la sottrazione di documenti con dati personali (furto, etc.).

2.1. SCOPO E AMBITO DI APPLICAZIONE

La procedura operativa descritta nel presente documento è finalizzata a definire in maniera chiara e comprensibile da tutto il personale aziendale interessato, il processo, le modalità operative, i ruoli e le responsabilità organizzative, che consentano un approccio esaustivo ed omogeneo nella gestione delle violazioni di sicurezza afferenti alla privacy, secondo i criteri e i principi stabiliti dalle vigenti normative.

2.2. ACRONIMI E DEFINIZIONI

Agente malevolo - Soggetto che, sfruttando eventuali vulnerabilità di sicurezza logica, fisica o organizzativa, ovvero abusando dei poteri e delle conoscenze derivanti dal proprio ruolo, compie, volontariamente o accidentalmente, atti che comportano una violazione della riservatezza, dell'integrità e della disponibilità degli asset afferenti ai sistemi informativi aziendali preposti al trattamento di dati personali.

Allarme di sicurezza – Segnalazione formalmente referenziata derivante dal rilevamento di uno o più eventi che rappresentano una presunta violazione della privacy.

Analisi post incidente - Insieme di attività finalizzate alla raccolta ed alla analisi delle evidenze utili a stabilire le cause, il contesto e le modalità di attuazione di una violazione della privacy.

Asset Informativo - Insieme definito, individuato e univocamente referenziabile, dei processi, delle informazioni, dei dati, delle infrastrutture tecnologiche hardware e software che costituiscono parte integrante dei trattamenti sottoposti alle norme ed ai regolamenti privacy.

Criticità - Insieme di circostanze avverse derivanti dalla concomitanza di eventi che costituiscono una minaccia per la sicurezza e la privacy di un determinato contesto.

Dominio di monitoraggio - Insieme definito di asset sottoposti al rilevamento e controllo sistematico degli eventi che si verificano durante il periodo di osservazione.

Escalation (dell'incidente) - Attività procedurale predefinita, che stabilisce e regolamenta le modalità di trasferimento di responsabilità nella gestione delle violazioni della privacy, in funzione di specifici parametri che ne definiscono le soglie di gravità e di criticità.

Evento di sicurezza - Qualsiasi occorrenza che si verifica nell'ambito di un determinato asset informativo, rilevata mediante strumenti automatizzati o non automatizzati, la cui valenza è considerata significativa ai fini delle attività di gestione, controllo della sicurezza e contenimento dei rischi ad essa correlati.

Evento critico - Qualsiasi evento significativo che, a seguito delle analisi effettuate dal personale incaricato, potrebbe sottintendere, direttamente o indirettamente, una violazione della privacy e/o delle politiche di

sicurezza logica, fisica ed organizzativa, applicate al sistema informativo preposto al trattamento di dati personali.

Falso positivo - Evento o insieme di eventi che, pur essendo stati segnalati come manifestazioni di possibili violazioni della privacy, non rivestono carattere di rilevanza nello specifico contesto entro il quale si sono verificati.

Incidente di sicurezza - Qualsiasi evento o insieme di eventi che sottintendono una violazione delle politiche di sicurezza ICT fonte di danno per gli asset ICT ovvero per il patrimonio informativo dell'Organizzazione.

Incidente Privacy - Un incidente di sicurezza che comporta violazioni della privacy in grado di arrecare gravi rischi per i diritti e le libertà del/degli Interessato/i.

Monitoraggio degli eventi di sicurezza - Insieme di attività continuative, organizzate, controllate e documentate, finalizzate al tracciamento, al rilevamento ed alla gestione degli eventi di sicurezza, anche con l'ausilio di strumenti automatici.

Minacce - Circostanze o eventi indesiderati, che possono determinare una violazione della sicurezza e della privacy.

Potenziale di aggressività della minaccia - Indicatore valutativo che esprime la pericolosità intrinseca della minaccia, indipendentemente dal contesto in cui questa può verificarsi.

Rischio di sicurezza - Misurazione quantitativa e/o qualitativa che esprime la possibilità che un determinato agente di minaccia possa causare una violazione della sicurezza ovvero arrecare un danno al patrimonio informativo, sfruttando una o più vulnerabilità insite in uno o più asset.

Violazione di sicurezza - Azione o insieme di azioni intenzionali o accidentali, intraprese da un agente malevolo, che comportano l'elusione o l'inibizione di una o più misure logiche, fisiche e organizzative, preposte alla tutela della sicurezza e della privacy.

Vulnerabilità - Elemento caratteristico di un determinato asset, che potrebbe essere sfruttato da agenti malevoli per apportare una violazione della sicurezza e della privacy.

2.3. DOCUMENTI DI RIFERIMENTO

[1] Regolamento (UE) 679/2016 (GDPR) – Considerando n.85, 86, 87, 88, artt. 33 e 34;

[2] Garante Privacy: Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. *data breach*) - 4 aprile 2013;

[3] Garante Privacy: Provvedimento generale prescrittivo in tema di biometria - 12 novembre 2014;

[4] Garante Privacy: Linee guida in materia di Dossier sanitario - 4 giugno 2015;

[5] Garante Privacy: Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche - 2 luglio 2015;

[6] Guidelines on Personal data breach notification under Regulation 2016/679 – article 29 data protection working party (Adopted on 3 October 2017 – as last Revised and Adopted on 6 February 2018).

2.4. GLOSSARIO

Acronimo/Definizione	Descrizione
GDPR	General Data Protection Regulation
RAT	Registro delle Attività di Trattamento
DPIA	Data Protection Impact Analysis
DPO	Data Processor Officer
RPD	Responsabile della Protezione dei Dati

2.5. COS'È UNA VIOLAZIONE DEI DATI PERSONALI (*DATA BREACH*)

Una violazione di dati personali o qualsiasi infrazione relativa alla sicurezza degli stessi che comporti - 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 dal Titolare del trattamento. Le violazioni di dati personali possono accadere per un ampio numero di ragioni che possono includere:

- divulgazione di dati confidenziali a persone non autorizzate;
- perdita o furto di dati o di strumenti nei quali i dati sono memorizzati;
- perdita o furto di documenti cartacei;
- infedeltà aziendale (ad esempio: *data breach* causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico);
- accesso abusivo (ad esempio: *data breach* causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite);
- casi di pirateria informatica;
- banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo "owner";
- virus o altri attacchi al sistema informatico o alla rete aziendale;
- violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o archivi, contenenti informazioni riservate);
- smarrimento di pc portatili, devices o attrezzature informatiche aziendali;
- invio di e-mail contenenti dati personali e/o particolari a erroneo destinatario.

2.6. A CHI SONO RIVOLTE QUESTE PROCEDURE

Queste procedure sono rivolte a tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza del Titolare del trattamento (meglio descritti al punto successivo della presente procedura) quali:

- i lavoratori dipendenti, nonché coloro che a qualsiasi titolo - e quindi a prescindere dal tipo di rapporto intercorrente - abbiano accesso ai dati personali trattati nel corso del proprio impiego per conto del Titolare del trattamento (di seguito genericamente denominati Destinatari interni);
- qualsiasi soggetto (persona fisica o persona giuridica) diverso dal Destinatario interno che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento abbia accesso ai suddetti dati e agisca in qualità di Responsabile del trattamento ex art. 28 GDPR o di autonomo Titolare (di seguito, genericamente denominati "Destinatari").

Tutti i Destinatari devono essere debitamente informati dell'esistenza della presente procedura, mediante metodi e mezzi che ne assicurino la comprensione.

Il rispetto della presente procedura è obbligatorio per tutti i soggetti coinvolti e la mancata conformità alle regole comportamentali (o di comportamento), previste dalla stessa potrà comportare provvedimenti disciplinari a carico dei dipendenti inadempienti ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia.

2.7. TIPI DI DATI CUI SI RIFERISCONO QUESTE PROCEDURE

Queste procedure si riferiscono a:

- dati personali trattati "da" e "per conto" del Titolare del trattamento, in qualsiasi formato (inclusi documenti cartacei) e con qualsiasi mezzo;
- dati personali conservati o trattati a mezzo di qualsiasi altro sistema aziendale.

Per «dato personale» si intende: *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*.

2.8. GESTIONE COMUNICAZIONE DI DATA BREACH

Le violazioni di dati personali sono gestite dal Titolare del trattamento o da un suo delegato, sotto la supervisione del RPD/DPO (qualora presente). In caso di concreta, sospetta e/o avvenuta violazione dei dati personali, è di estrema importanza assicurare che la stessa sia affrontata immediatamente e correttamente al fine di minimizzare l'impatto della violazione e prevenire che si ripeta. Nel caso in cui uno dei Destinatari si accorga di una concreta, potenziale o sospetta violazione dei dati personali, dovrà immediatamente informare dell'incidente il superiore gerarchico il quale si occuperà, con il supporto dei Destinatari stessi, di informare il Titolare del trattamento o un suo delegato mediante la compilazione dell'**Allegato A – Modulo di comunicazione interna di *Data Breach*** da inviare a mezzo mail al Titolare del trattamento.

2.9. GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI

Per gestire una violazione dei dati personali è necessario seguire i seguenti quattro step:
Step 1: Identificazione e indagine preliminare;
Step 2: Contenimento, recovery e risk assessment;
Step 3: Eventuale notifica all'Autorità Garante;
Step 4: Eventuale comunicazione agli interessati;
Step 5: Documentazione della violazione.

Step 1: Identificazione e indagine preliminare

L'**Allegato A**, debitamente compilato, permetterà al Titolare del trattamento o un suo delegato, di condurre una valutazione iniziale riguardante la notizia dell'incidente occorso, ciò al fine di stabilire se si sia effettivamente verificata un'ipotesi di *Data Breach* (violazione) e se sia necessaria un'indagine più approfondita dell'accaduto, procedendo con il risk assessment (step 2) e con il coinvolgimento del RPD/DPO, ove presente.

Nel caso in cui si tratti di violazione di dati contenuti in un sistema informatico, il Titolare del trattamento o un suo delegato dovrà coinvolgere in tutta la procedura indicata nel presente documento anche il Responsabile dell'Ufficio IT o un suo delegato in caso di assenza.

Detta valutazione iniziale sarà effettuata attraverso l'esame delle informazioni riportate nell'**Allegato A**, quali:

- la data di scoperta della violazione (tempestività);
- il soggetto che è venuto a conoscenza della violazione;
- la descrizione dell'incidente (natura della violazione e dei dati coinvolti);
- le categorie e il numero approssimativo degli interessati coinvolti nella violazione;
- la descrizione di eventuali azioni già poste in essere.

Step 2: Contenimento, Recovery e risk assessment

Una volta stabilito che si è verificato un *Data Breach*, il Titolare del trattamento o un suo delegato insieme al RPD/DPO, se presente, dovranno stabilire:

a) se esistono azioni che possano limitare i danni che la violazione potrebbe causare (es. riparazione fisica di strumentazione, utilizzo dei file di back up per recuperare dati persi o danneggiati, isolamento/chiusura di un settore compromesso della rete, cambio dei codici di accesso, etc.);
b) una volta identificate tali azioni, quali siano i soggetti che devono agire per contenere la violazione;
c) se sia necessario notificare la violazione all'Autorità Garante per la Protezione dei dati personali (ove sia probabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche);
d) se sia necessario comunicare la violazione agli interessati (ove la violazione presenti un elevato rischio per i diritti e le libertà delle persone fisiche).

Al fine di individuare la necessità di notificare all'Autorità Garante e di comunicazione agli interessati, il Titolare del trattamento e il RPD/DPO valuteranno la gravità della violazione utilizzando l'**Allegato B - Modulo di valutazione del Rischio connesso al *Data Breach*** che dovrà essere esaminato unitamente all'**Allegato A**, tenendo, altresì, in debita considerazione i principi e le indicazioni di cui all'art. 33 del GDPR.

Se, infatti, gli obblighi di notifica all'Autorità di Controllo scaturiscono dal superamento di una soglia di rischio semplice, l'art. 34 del GDPR prevede, invece, che l'obbligo di comunicazione agli interessati sia innescato dal superamento di un rischio elevato.

Step 3: Eventuale notifica all'Autorità Garante competente

Una volta valutata la necessità di effettuare la notifica della violazione dei dati subita sulla base della procedura di cui allo step 2, secondo quanto prescritto dal Regolamento (UE) 2016/679, il Titolare del trattamento, dovrà provvedervi, senza ingiustificato ritardo e, ove possibile **entro 72 ore** dal momento in cui ne è venuta a conoscenza.

Pertanto, il Titolare del trattamento e il RPD/DPO (qualora presente) individueranno l'Autorità di Controllo competente sulla base delle informative e/o della valutazione d'impatto sulla protezione dei dati, in relazione ai dati oggetto di violazione (in mancanza di tale documentazione che abbia preventivamente individuato l'Autorità

Garante competente, la stessa sarà da individuare in quella dello Stato in cui è ubicato lo stabilimento principale o lo stabilimento unico del Titolare del trattamento, anche per i trattamenti transfrontalieri eventualmente effettuati).
Una volta determinata l'Autorità di Controllo competente, il Titolare del trattamento e il RPD/DPO (qualora presente) individueranno la corretta modulistica da utilizzare per effettuare la notificazione e vi provvederanno.

Step 4: Eventuale comunicazione agli interessati

Una volta valutata la necessità di effettuare la comunicazione della violazione dei dati a coloro dei cui dati si tratta, sulla base della procedura di cui allo step 2, secondo quanto prescritto dal Regolamento (UE) 2016/679, il Titolare del trattamento, dovrà provvedervi, senza ingiustificato ritardo. Quanto al contenuto di tale comunicazione, il Titolare del trattamento o da un suo delegato e il RPD/DPO dovranno:

- comunicare il nome e i dati di contatto del Responsabile della protezione dei dati (DPO);
- descrivere le probabili conseguenze della violazione dei dati personali;
- 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, se del caso, per attenuarne i possibili effetti negativi.

Quanto alle modalità di comunicazione, caso per caso, il Titolare del trattamento o un suo delegato e il RPD/DPO dovranno sempre privilegiare la modalità di comunicazione diretta con i soggetti interessati (quali e-mail, SMS o messaggi diretti). Il messaggio dovrà essere comunicato in maniera evidente e trasparente, evitando quindi di inviare le informazioni nel contesto di update generali o newsletter, che potrebbero essere facilmente fraintesi dai lettori. Nel caso in cui la segnalazione diretta richieda uno sforzo ritenuto sproporzionato, allora si potrà utilizzare una comunicazione pubblica, che dovrà essere ugualmente efficace nel contatto diretto con l'interessato.

Step 5: Documentazione della violazione

Indipendentemente dalla valutazione circa la necessità di procedere a notificazione e/o comunicazione della violazione di *Data Breach*, ogni qualvolta si verifichi un incidente comunicato dai Destinatari attraverso l'**Allegato A**, il Titolare del trattamento, sarà tenuta a documentarlo. Tale documentazione sarà affidata al Titolare del trattamento o da un suo delegato con l'ausilio del Responsabile dell'Ufficio IT (qualora la violazione riguardi dati contenuti in sistemi informatici) vi provvederà mediante la tenuta dell'**Allegato C - Registro dei Data Breach**, secondo le informazioni ivi riportate:

- n. violazione;
- data violazione;
- natura della violazione;
- categoria di interessati;
- categoria di dati personali coinvolti;
- numero approssimativo di registrazioni dei dati personali;
- conseguenze della violazione;
- contromisure adottate;
- se sia stata effettuata notifica all'Autorità Garante Privacy;
- se sia stata effettuata comunicazione agli interessati.

Il Registro dei *Data Breach* deve essere continuamente aggiornato e messo a disposizione del Garante qualora l'Autorità chieda di accedervi.

3. RUOLI E RESPONSABILITÀ

La tabella seguente riepiloga e descrive i ruoli e le responsabilità, descritte mediante una matrice, dei soggetti coinvolti nel processo di gestione delle violazioni della sicurezza con impatti sulla privacy.

RUOLI E RESPONSABILITÀ NEL PROCESSO DI GESTIONE DELLE VIOLAZIONI DI SICUREZZA CON IMPATTI SULLA PRIVACY		
Soggetto	*Ruolo assegnato dalla procedura*	*Responsabilità (RACI)*
TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI	Ruolo istituzionale a cui è attribuita la Titolarità degli adempimenti di legge previsti per la gestione degli incidenti (*data breach*).	Accountable – supervisione delle attività ed approvazione dei documenti prodotti nelle fasi di gestione degli incidenti con impatti privacy.
DATA PROTECTION OFFICER	Ruolo istituzionale che fornisce il supporto tecnico al Titolare del trattamento, per il corretto indirizzamento delle decisioni intraprese nel corso del processo di gestione degli incidenti con impatti sulla privacy.	Collaborate – Supporto alle decisioni intraprese dal Titolare del trattamento. Responsabile per il coordinamento della gestione e trattamento degli incidenti.
RESPONSABILE DELLA GESTIONE DEGLI INCIDENTI	Ruolo aziendale responsabile del coordinamento di tutto il processo di gestione delle violazioni di sicurezza con impatti sulla privacy.	Responsabile del coordinamento del processo di gestione delle violazioni di sicurezza con impatti sulla privacy.
OPERATORI DELLA SICUREZZA ICT	Personale tecnico delle unità Operative ICT incaricato dello svolgimento delle attività di monitoraggio, rilevamento degli eventi e classificazione degli allarmi di sicurezza ICT con impatti sulla privacy.	Collaborate – Collabora, sotto il riporto funzionale del Responsabile della gestione degli incidenti, nello svolgimento delle attività operative di monitoraggio, analisi eventi, classificazione e gestione degli allarmi di sicurezza ICT con impatti sulla privacy.

3.1. DATA BREACH PRESSO UN SOGGETTO IN QUALITÀ DI RESPONSABILE A. OBBLIGHI DI COMUNICAZIONE DELLA SOCIETÀ QUANDO OPERA IN QUALITÀ DI RESPONSABILE

Quando un soggetto terzo agisce in qualità Responsabile subisca una Violazione dei Dati Personali trattati per conto del Titolare, deve informare quest'ultimo (solitamente il cliente per il quale offre servizi), senza ingiustificato ritardo secondo i tempi e i modi concordati nel contratto per il trattamento dei dati personali trasmesso da quest'ultimo (o in quelli concordati nel Contratto per il Trattamento dei Dati Personali).

3.2. ATTI PENALMENTE RILEVANTI

Il titolare, in accordo con il RPD/DPO se presente, potrà costituire un team di esperti nelle aree di competenza necessarie, col compito di verificare la fondatezza delle circostanze rappresentate nella segnalazione. Il team effettuerà quindi ogni attività che il Titolare e l'RPD/DPO se presente riterrà opportuna, inclusa l'audizione personale del segnalante e di eventuali altri soggetti che possono riferire sui fatti segnalati, nel rispetto dei principi di imparzialità e riservatezza. Nel report saranno incluse le misure correttive necessarie da adottare e si procederà quindi alla segnalazione al Garante della Privacy nel termine di **72 ore**.

4. MODALITÀ DI COMUNICAZIONE AGLI INTERESSATI

Nel caso in cui dal *data breach* possa derivare un rischio elevato per i diritti e le libertà delle persone, anche quest'ultime devono essere informate senza ingiustificato ritardo, al fine di consentire loro di prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione. Il referente privacy 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 RPD/DPO (qualora presente), individuerà come più opportuna ai sensi dell'art. 34 del GDPR e tenendo conto di eventuali indicazioni fornite dall'Autorità Garante.

Versione 001 del 28 gennaio 2020

ALLEGATO A

MODELLO PER LA COMUNICAZIONE DELLA VIOLAZIONE DEI DATI DAL RESPONSABILE AL TITOLARE (AI FINI DEL C.D. "DATA BREACH")

(da inviare tramite PEC tempestivamente all'indirizzo PEC del Titolare del trattamento e all'indirizzo PEC del Responsabile per la protezione dei dati)

DATI DEL RESPONSABILE DEL TRATTAMENTO

FORMA GIURIDICA **STUDIO GADLER SRL**		
CODICE FISCALE **01839270228**		
P. IVA **01839270228**		
SEDE LEGALE IN		
C.A.P. **38057**	COMUNE **PERGINE VALSUGANA**	PROV. **TN**
INDIRIZZO **VIA GRABERI**		N. **12/A**
TELEFONO FISSO **0461/512522**		
E-MAIL **DPO@STUDIOGADLER.IT**		
PEC **PEC.GADLER@PEC.GADLER.IT**		
ALTRO DOMICILIO ELETTRONICO PER INVIO DELLE COMUNICAZIONI INERENTI **/**		

REFERENTI DEL RESPONSABILE DEL TRATTAMENTO

NOME E COGNOME **GIOVANNI POLETTO**	
CODICE FISCALE **PLTGNN73S07B006D**	
TELEFONO **0461/512522**	CELLULARE **348/9969677**
E-MAIL **DPO@STUDIOGADLER.IT**	
PEC **PEC.GADLER@PEC.GADLER.IT**	

Denominazione della/e banca/banche dati oggetto di *data breach* e breve descrizione della violazione dei dati personali ivi trattati

Quando si è verificata la violazione dei dati personali trattati nell'ambito della banca dati?

☐ Il _____

☐ Tra il _____ e il _____

☐ In un tempo non ancora determinato.

☐ È possibile che sia ancora in corso.

Dove è avvenuta la violazione dei dati?

(specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

_____

_____

_____

Modalità di esposizione al rischio - Tipo di violazione

☐ Lettura (presumibilmente i dati non sono stati copiati)

☐ Copia (i dati sono ancora presenti sui sistemi del Titolare)

☐ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)

☐ Cancellazione (i dati non sono più sui sistemi del Titolare e non li ha neppure l'autore della Violazione)

☐ Furto (i dati non sono più sui sistemi del Titolare e li ha l'autore della violazione)

☐ Altro (specificare):

_____

_____

_____

Dispositivo oggetto della violazione

☐ Computer

☐ Rete

☐ Dispositivo mobile

☐ File o parte di un file

☐ Strumento di backup

☐ Documento cartaceo

☐ Altro (specificare):

_____

_____

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione:

_____

_____

Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati?

☐ N. _____ persone
☐ Circa _____ persone
☐ Un numero (ancora) sconosciuto di persone

Che tipo di dati sono oggetto di violazione?

☐ Dati anagrafici/codice fiscale
☐ Dati di accesso e di identificazione (user name, password, customer ID, altro)
☐ Dati relativi a minori
☐ Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale
☐ Dati personali idonei a rivelare lo stato di salute e la vita sessuale
☐ Dati giudiziari
☐ Copia per immagine su supporto informatico di documenti analogici
☐ Ancora sconosciuto
☐ Altro (specificare):

_____

_____

_____

Livello di gravità della violazione dei dati personali trattati nell'ambito della banca dati (secondo le valutazioni del Titolare)?

☐ Basso/trascurabile
☐ Medio
☐ Alto
☐ Molto alto

Misure tecniche e organizzative applicate ai dati oggetto di violazione

Si ritiene che la violazione vada comunicata anche agli interessati?

Sì, perché _____

No, perché _____

Qual è il contenuto della comunicazione da rendere agli interessati?

_____

_____

Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?

Luogo e data _____ Firma leggibile _____

ALLEGATO B

MODULO DI VALUTAZIONE DEL RISCHIO CONNESSO AL *DATA BREACH*

VALUTAZIONE /ACCERTAMENTO ASSESSMENT DI GRAVITÀ	A CURA DEL RPD/DPO INSIEME CON L'UFFICIO IT E IL RESPONSABILE DELL'UFFICIO COINVOLTO DELLA VIOLAZIONE
Dispositivi oggetto del *Data Breach* (computer, rete dispositivo mobile, file o parte di un file, strumento di back up, documento cartaceo, altro):	
Modalità di esposizione al rischio (tipo di violazione): • lettura (presumibilmente i dati non sono stati copiati) • copia (i dati sono ancora presenti sui sistemi ma del titolare) • alterazione (i dati sono presenti sui sistemi ma sono stati alterati) • cancellazione (i dati non sono più presenti e non li ha neppure l'autore della violazione) • furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione) • altro	
Breve descrizione dei sistemi di elaborazione o di memorizzazione dati coinvolti, con indicazione della loro ubicazione:	
Se laptop/portatile è stato perso/rubato: Quando è stata l'ultima volta in cui il laptop è stato sincronizzato con il sistema IT centrale?	
Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati violata?	
La violazione può avere conseguenze negative in uno dei seguenti settori aziendali:	
Qual è la natura dei dati coinvolti? (compilare le sezioni sottostanti)	
I dati particolari (come identificati dal Regolamento (UE) 2016/679 relative ad una persona viva ed individuabile: • origine razziale o etnica • opinion politiche, convinzioni religiose o filosofiche • appartenenza sindacale • dati genetici • dati biometrici • dati giudiziari/penali • relative alla salute o all'orientamento sessuale di una persona	

Informazioni che possono essere utilizzate per commettere furti d'identità: (ad esempio, dati di accesso e di identificazione, codice fiscale e copie di carta d'identità, passaporto o carte di credito)	
Informazioni personali relative a soggetti fragili: (ad esempio, anziani, disabili, minori)	
Profili individuali che includono informazioni relative a performance lavorative, salario o stato di famiglia, sanzioni disciplinari, che potrebbero causare danni significativi alle persone:	
Altro:	
La violazione può comportare pregiudizio alla reputazione, perdita di riservatezza di dati protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro dato economico o sociale significativo?	
Gli interessati rischiano di essere privati dell'esercizio del controllo sui dati personali che li riguardano?	
Quali misure tecniche e organizzative sono adottate ai dati oggetto di violazione? (ad es., la pseudonimizzazione e la cifratura dei dati personali)	
Il Titolare del trattamento ha aderito ad un codice di condotta approvato ai sensi dell'art. 40 Regolamento (UE) o un meccanismo di certificazione di cui all'art. 42 Regolamento (UE)?	
Il Titolare del trattamento ha adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati successivamente alla violazione?	
Classificazione della violazione (1, 2 o 3) e motivazioni:	
Notificazione del *Data Breach* all'Autorità Garante	SI/NO: Se sì, notificato in data: Dettagli:
Comunicazione del *Data Breach* agli interessati	SI/NO: Se sì, notificato in data: Dettagli:
Comunicazione del *Data Breach* ad altri soggetti **(ad es., casa madre)**	SI/NO: Se sì, notificato in data: Dettagli: