Battistolli Servizi Integrati S.r.l.
Sede Legale: Via Basilio dalla Scola 88 - 36100 VICENZA
Tel. 0444 302128 - Fax 0444 394678
C.F. - Reg. Impr.e P.IVA 03897120246 - R.E.A. VI - 363178
Cap. Soc. € 100.000,00 i.v.

PROCEDURA DI GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI

in applicazione del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati

Battistolli Servizi Integrati S.r.l.
Sede Legale: Via Basilio dalla Scola 88 - 36100 VICENZA
Tel. 0444 302128 - Fax 0444 394678
C.F. - Reg. Impr.e P.IVA 03897120246 - R.E.A. VI - 363178
Cap. Soc. € 100.000,00 i.v.

INDICE

1. PREMESSE

Battistolli Servizi Integrati s.r.l. (di seguito, anche, "**Titolare**" o "**Azienda**") è tenuta, ai sensi
(i) del Regolamento Generale sulla Protezione dei Dati – Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito "**GDPR**") e
(ii) del D. Lgs. n. 196/2003 recante il "Codice in materia di protezione dei dati personali" integrato con le modifiche introdotte dal D. Lgs. n. 101/2018 (di seguito "**Codice**"),
di seguito, congiuntamente, "**Normativa sulla protezione dei dati personali**",
a mantenere sicuri i dati personali trattati nell'ambito delle proprie attività e ad agire senza ingiustificato ritardo in caso di violazione dei dati stessi (incluse eventuali notifiche all'Autorità Garante competente ed eventuali comunicazioni agli interessati).
È di fondamentale importanza predisporre azioni da attuare nell'eventualità in cui si presentino violazioni presunte, potenziali o effettive di dati personali, ciò al fine di evitare rischi per i diritti e le libertà degli interessati, nonché danni economici all'Azienda e per poter riscontrare nei tempi e nei modi previsti dal GDPR l'Autorità Garante e/o gli interessati.

2. SCOPO

Lo scopo della presente procedura è di definire il flusso di attività per la gestione delle violazioni dei dati personali trattati dal Titolare.

3. DESTINATARI

La presente procedura è rivolta a tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza del Titolare 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 (di seguito "**Destinatari interni**");
- qualsiasi soggetto (persona fisica o persona giuridica) diverso dai Destinatari interni che, in ragione del rapporto contrattuale in essere con il Titolare abbia accesso ai suddetti dati e agisca in qualità di Responsabile del trattamento ex art. 28 del GDPR o di autonomo Titolare del trattamento (di seguito "**Destinatari esterni**"),

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.

4. DEFINIZIONI

- *dato personale*, qualsiasi informazione riguardante una persona fisica identificata o identificabile; 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 (di seguito "**Dato Personale**");
- *trattamento*, qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati ed applicate ai 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 (di seguito "**Trattamento**");
- *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 (di seguito "**Titolare del trattamento**");

- *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 (di seguito "**Responsabile**");
- *interessato*, qualsiasi persona fisica identificata o identificabile (di seguito "**Interessato**");
- *data protection officer* o *responsabile della protezione dei dati*, è un consulente tecnico designato dal titolare del trattamento, le cui competenze sono disciplinate dal GDPR (di seguito "**DPO**" o "**RPD**");
- *team privacy*, è un gruppo di persone nominate dal Titolare con la funzione di:
  (i) effettuare, anche con l'ausilio di consulenti esterni nominati dall'Azienda, tutte le attività inerenti e necessarie per la *compliance* alla Normativa sulla protezione dei dati personali;
  (ii) gestire il Modello Organizzativo Privacy adottato dal Titolare;
  (iii) relazionarsi con il DPO
  (di seguito "**Team privacy**");
- *autorità di controllo*, l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR (per l'Italia tale autorità si identifica con il "Garante per la protezione dei dati personali") (di seguito "**Autorità**");
- *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 (di seguito "**Violazione**" o "**Data Breach**").

Le Violazioni possono accadere per varie ragioni che possono includere a titolo esemplificativo:

- 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.

5. GESTIONE DELLA COMUNICAZIONE DI VIOLAZIONE

Le Violazioni sono gestite dal Titolare con l'ausilio del Team privacy e con la supervisione del DPO.
Nello specifico il Team privacy e il DPO hanno il compito di coadiuvare il Titolare nella risoluzione delle questioni relative a un evento di Data Breach sospetto, presunto o effettivo, esprimendosi in relazione ai seguenti aspetti (esemplificativi e non esaustivi) ove applicabili:

1. determinare se la violazione di cui trattasi debba o meno essere considerata una Violazione;
2. assegnare un livello di gravità alla Violazione;
3. assicurare che sia avviata, condotta, documentata e conclusa un'indagine corretta e imparziale;
4. identificare i requisiti per la risoluzione della Violazione e monitorare la soluzione;
5. coordinarsi con l'Autorità;
6. coordinare le comunicazioni interne ed esterne;
7. assicurarsi che gli interessati siano adeguatamente informati.

Se ritenuto opportuno e necessario, all'esito delle prime analisi condotte in merito al potenziale grado di gravità nonché di specificità della Violazione, il Titolare, sentito anche il Team privacy e il DPO, può coinvolgere nelle

attività di gestione del Data Breach anche ulteriori esperti esterni (a titolo esemplificativo un esperto di sicurezza informatica o un'agenzia di comunicazione esterna per assistere il Titolare in caso di necessità di comunicazione a terzi).

In caso di sospetta, presunta o effettiva Violazione, è di estrema importanza assicurare che la stessa sia affrontata immediatamente e correttamente al fine di minimizzare l'impatto della Violazione e prevenire una sua eventuale ripetizione.

Nel caso in cui uno dei Destinatari si accorga di una sospetta, presunta o effettiva Violazione, dovrà darne immediata comunicazione come segue:

(i) se è un Destinatario interno, al proprio responsabile di area/funzione il quale si occuperà, con il supporto dei destinatari stessi, di informare il Titolare mediante la compilazione dell'Allegato **A** – "Modulo di comunicazione di Data Breach" da inviare a mezzo mail all'indirizzo odv.bsi@battistolli.it;

(ii) se è un Destinatario esterno, informa il Titolare senza ingiustificato ritardo mediante la compilazione dell'Allegato **A** – "Modulo di comunicazione esterna di Data Breach" da inviare a mezzo mail all'indirizzo odv.bsi@battistolli.it.

6. PROCESSO DI GESTIONE DELLA VIOLAZIONE

Per gestire una violazione dei dati personali è necessario seguire i seguenti step:
Step 1: Identificazione e indagine preliminare
Step 2: Contenimento, recupero dei dati e risk assessment
Step 3: Eventuale notifica all'Autorità
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, con l'ausilio del Team privacy e con il supporto del DPO, di condurre una valutazione iniziale riguardante la comunicazione ricevuta, ciò al fine di stabilire se si sia effettivamente verificata un'ipotesi di Data Breach e se sia necessaria un'indagine più approfondita dell'accaduto, procedendo in tal caso con lo step 2.
Nel caso in cui si tratti di violazione di dati contenuti in un sistema informatico, il Titolare dovrà coinvolgere in tutta la procedura indicata nel presente documento anche il Responsabile IT o un suo delegato in caso di assenza.

Step 2: Contenimento, recupero dei dati e risk assessment
Una volta stabilito che un Data Breach è avvenuto, il Titolare insieme al Team privacy e al DPO dovranno stabilire:

- se esistono azioni che possano limitare i danni che la Violazione potrebbe causare (i.e. 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… ecc.);
- una volta identificate tali azioni, quali siano i soggetti che devono agire per contenere la Violazione;
- se sia necessario notificare la Violazione all'Autorità (ove sia probabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche);
- se sia necessario comunicare la violazione agli interessati (ove la violazione presenti un rischio elevato per i diritti e le libertà delle persone fisiche).

Al fine di individuare la necessità di notificazione all'Autorità e di comunicazione agli interessati, il Titolare, coadiuvato dal Team privacy e dal DPO, valuterà la gravità della Violazione utilizzando un apposito "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 agli artt. 33 e 34 del GDPR.

Step 3: Eventuale notifica all'Autorità

Una volta valutata la necessità di effettuare la notifica della Violazione subita all'Autorità sulla base della procedura di cui allo step 2, secondo quanto prescritto dal GDPR, il Titolare dovrà provvedervi, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza.
Qualora la notifica all'Autorità non sia effettuata entro 72 ore, la comunicazione dovrà essere corredata anche dei motivi del ritardo.

La notifica dovrà almeno:

a) descrivere la natura della Violazione 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 o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della Violazione;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare per porre rimedio alla Violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora e nella misura in cui non fosse possibile fornire le informazioni contestualmente, le informazioni potranno essere fornite all'Autorità in fasi successive senza ulteriore ingiustificato ritardo.

Step 4: Eventuale comunicazione agli Interessati
Una volta valutata la necessità di effettuare la comunicazione della Violazione agli Interessati sulla base della procedura di cui allo step 2, secondo quanto prescritto dal GDPR, il Titolare dovrà provvedervi, senza ingiustificato ritardo.
La comunicazione agli Interessati dovrà essere scritta in un linguaggio chiaro e semplice e dovrà contenere:

a) il nome e i dati di contatto del DPO o di altro punto di contatto presso cui ottenere più informazioni;
b) la descrizione delle probabili conseguenze della Violazione;
c) la descrizione delle le misure adottate o di cui il Titolare propone l'adozione per porre rimedio alla Violazione e, se del caso, per attenuarne i possibili effetti negativi.

Quanto alle modalità di comunicazione, caso per caso, il Titolare dovrà sempre privilegiare la modalità di comunicazione diretta con i soggetti interessati (quali email, SMS o messaggi diretti). Il messaggio dovrà essere comunicato in maniera semplice e trasparente, evitando quindi di inviare le informazioni nel contesto di newsletter, che potrebbero essere facilmente fraintese dagli Interessati. 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 necessità di procedere alla notificazione all'Autorità (step 3) e/o alla comunicazione agli Interessati (step 4) della Violazione, ogni qualvolta sia comunicato dai Destinatari un potenziale Data Breach attraverso l'allegato A, il Titolare è tenuto a documentarlo.
Tale attività di documentazione sarà attuata mediante la tenuta a cura del Titolare, con l'ausilio del Team privacy, di un apposito "Registro delle violazione dei dati personali".
Il Registro delle violazione dei dati personali deve essere continuamente aggiornato e messo a disposizione dell'Autorità qualora chieda di accedervi.

7. RESPONSABILIZZAZIONE

Il rispetto della presente procedura è obbligatorio per tutti i Destinatari e la mancata conformità a quanto previsto 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.

8. PERIODO DI CONSERVAZIONE DELLE REGISTRAZIONI SULLA BASE DEL PRESENTE DOCUMENTO

Documento	Base giuridica del trattamento	Periodo di conservazione
Moduli di comunicazione interna ed esterna di Data Breach	(Art. 6, comma 1, lett. c), GDPR) Trattamento necessario per adempiere un obbligo legale al quale è soggetto il Titolare (Art. 6, comma 1, lett. f), GDPR) Trattamento necessario per il perseguimento del legittimo interesse del Titolare connesso alla gestione della propria organizzazione	Permanente
Decisioni documentate del Titolare in merito alla Violazione	(Art. 6, comma 1, lett. c), GDPR) Trattamento necessario per adempiere un obbligo legale al quale è soggetto il Titolare (Art. 6, comma 1, lett. f), GDPR) Trattamento necessario per il perseguimento del legittimo interesse del Titolare connesso alla gestione della propria organizzazione	5 anni
Comunicazione di una Violazione	(Art. 6, comma 1, lett. c), GDPR) Trattamento necessario per adempiere un obbligo legale al quale è soggetto il Titolare (Art. 6, comma 1, lett. f), GDPR) Trattamento necessario per il perseguimento del legittimo interesse del Titolare connesso alla gestione della propria organizzazione	5 anni
Registro delle violazioni di dati personali	(Art. 6, comma 1, lett. c), GDPR) Trattamento necessario per adempiere un obbligo legale al quale è soggetto il Titolare (Art. 6, comma 1, lett. f), GDPR) Trattamento necessario per il perseguimento del legittimo interesse del Titolare connesso alla gestione della propria organizzazione	Permanente

9. GESTIONE DEL PRESENTE DOCUMENTO

Il responsabile di questo documento è il Titolare, il quale deve controllare il documento con frequenza almeno annuale e, ove necessario, provvedere alle eventuali modificazioni/aggiornamenti.

Allegati:

- "A - Modulo di comunicazione interna di Data Breach"

Allegato "**A**" – Modulo di comunicazione di Data Breach

Qualora sia rilevata una sospetta, presunta o effettiva violazione dei dati personali, è necessario darne immediata comunicazione al Titolare del trattamento mediante compilazione del modulo che segue da inviare a mezzo e-mail al seguente indirizzo: b.s.i.@legalmail.it

Comunicazione di Data Breach

Data di compilazione:	

□ **DESTINATARIO INTERNO ***

Dati della persona che fa la segnalazione:

Cognome e nome	
Incarico/Mansione	
Dati di contatto (indirizzo e-mail, numero di telefono)	

□ **DESTINATARIO ESTERNO ***

Dati del soggetto che fa la segnalazione:

Ditta\Ragione sociale	
Dati di contatto del DPO (ove nominato)	
Cognome e nome del soggetto segnalatore	
Dati di contatto (indirizzo e-mail, numero di telefono)	

* indicare, alternativamente, se il soggetto che fa la segnalazione è un Destinatario interno o un Destinatario esterno.

*****

DESCRIZIONE DELL'EVENTO

Data di scoperta della violazione (data, ora)	
Data e luogo della violazione (data, ora, luogo)	
Descrizione di cosa è successo	
Descrizione di come è successo	
Categorie e numero approssimativo di interessati coinvolti nella violazione	
Volume (anche approssimativo) di dati personali oggetto di violazione	
Altri dettagli rilevanti (eventuali azioni poste in essere al momento di scoperta della violazione ecc..)	

A cura del Titolare del trattamento (o del referente da esso incaricato)		**DATA E ORA RICEZIONE MODULO:**	
Modalità di ricezione:		N° Progressivo di segnalazione (da Registro Violazione Dati):	
Sistemi coinvolti:			
Vulnerabilità rilevate:			