POLICY DATA BREACH

NOVA GROUP SRL
Sede legale: Via Dante,7 Frattamaggiore(NA) 80027
p.iva:11173370963

Sommario

A. SCOPO DEL DOCUMENTO

Il presente documento è adottato da Nova Group S.r.l., P.IVA11173370963, con sede legale in Frattamaggiore (NA), alla via Dante, n. 7 (di seguito, la "Società") in conformità alla normativa applicabile in materia di protezione dei dati personali ed, in particolare, al GDPR 2016/679 (di seguito, "GDPR" o il "Regolamento").
Il presente documento ha lo scopo di chiarire e di fornire adeguate istruzioni sulle azioni da adottare in caso di realizzazione di un *data breach*.

B. AMBITO DI APPLICAZIONE

Il presente documento si applica all'Amministratore di Sistema e a tutti gli amministratori, dirigenti, collaboratori, stagisti e dipendenti della Società in quanto richiamati.

C. DEFINIZIONI

Amministratore di Sistema: il soggetto preposto a specifiche attività da svolgersi sui sistemi operativi del Titolare ai sensi del Provvedimento del Garante del 27 novembre 2008, e ss.mm.ii.
Autorità di Controllo: l'autorità pubblica indipendente istituita da ciascuno Stato membro dell'Unione europea ai sensi dell'articolo 51 del Regolamento;
Codice: Decreto legislativo 30 giugno 2003, n. 196 e ss.mm.ii. (cd. Codice in materia di protezione dei dati personali);
Data Breach: una qualsivoglia violazione di sicurezza 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 e che possa provocare danni fisici, materiali o immateriali agli Interessati, ad esempio perdita del controllo dei Dati Personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei Dati Personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata;
Dato Personale (o "**Dato**")**:** qualsiasi informazione riguardante una persona fisica identificata o identificabile (di seguito, "**Interessato**"). Si considera identificabile la persona fisica che può essere identificata, direttamente o anche soltanto 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;
Garante: Autorità di Controllo italiana, vale a dire il Garante per la protezione dei dati personali;
Responsabile del Trattamento (o "**Responsabile**")**:** il soggetto nominato dal Titolare del Trattamento che ha il compito di trattare i Dati per conto del Titolare, ponendo in essere tutte le azioni necessarie per la tutela dei Dati Personali, compreso il profilo della sicurezza, e seguendo le istruzioni impartite dal Titolare;

Responsabile della protezione dei dati (o "**DPO**"): persona fisica o persona giuridica eventualmente designata dal Titolare del Trattamento o dal Responsabile del Trattamento laddove ricorrano i presupposti indicati all'articolo 38 del GDPR, i cui incarichi sono determinati all'articolo 39 del GDPR.
Titolare del Trattamento (o "**Titolare**"): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che in conformità alle norme di legge, singolarmente o insieme ad altri, definisce le finalità e i mezzi (ad es. come raccogliere i Dati, dove conservarli, come e quando farne uso) del Trattamento dei Dati Personali;
Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, 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.

D. POLICY

1. Introduzione e criteri da utilizzare per la qualificazione dei Data Breach

Il Regolamento, all'art. 4 n. 12, definisce una Violazione dei Dati Personali, come una "*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*".
A mero titolo esemplificativo, ma non esaustivo, rientrano nella definizione di Data Breach:
• la perdita di un telefono cellulare aziendale sul quale è installata la casella di posta elettronica aziendale;
• la sottrazione di un *personal computer* aziendale;
• un accesso non autorizzato ai sistemi della Società;
• l'erronea cancellazione di un database aziendale;
• la condivisione con soggetti non autorizzati di una serie di Dati Personali degli Interessati.
In caso di Violazione dei Dati Personali:
• l'art. 33, paragrafo 1, del Regolamento impone al Titolare del Trattamento l'obbligo di notifica della Violazione dei Dati Personali all'Autorità di Controllo competente, senza ingiustificato ritardo;
• l'art. 33, paragrafo 2, del Regolamento impone al Responsabile del Trattamento, senza ingiustificato ritardo dopo essere venuto a conoscenza di una Violazione dei Dati Personali, l'obbligo di informare il Titolare del Trattamento.
Inoltre, l'art. 33, paragrafo 5, del Regolamento richiede inoltre che il Titolare del Trattamento documenti "*qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.*"
All'interno della Società – in virtù delle interpretazioni date in materia dal Garante e dalle altre Autorità di Controllo – le Violazioni dei Dati Personali devono essere classificate, documentate e riportate esternamente in base ai seguenti criteri:
• **Violazione della riservatezza**: in caso di divulgazione o accesso non autorizzato o accidentale ai Dati Personali;

• **Violazione della disponibilità**: in caso di perdita non autorizzata o accidentale o in caso di distruzione di Dati Personali;
• **Violazione dell'integrità**: in caso di alterazione non autorizzata o accidentale dei Dati Personali.

I suddetti criteri devono dunque essere tenuti in considerazione dai destinatari della presente procedura e, in particolare, dall'Amministratore di Sistema e dal DPO per la valutazione della Violazione dei Dati Personali verificatasi, sia essa concernente Dati personali per i quali la Società riveste il ruolo di Titolare del Trattamento (alla luce degli obblighi di *reporting* interno, di notifica all'Autorità di Controllo e/o di comunicazione agli Interessati), sia essa riguardante Dati Personali per i quali la Società riveste il ruolo di Responsabile del Trattamento (alla luce dell'obbligo di comunicazione nei confronti del Titolare del Trattamento).

In aggiunta a quanto sopra considerato, la Società identifica ed adotta precisi strumenti e determinate linee guida, da attuare e seguire in caso di Violazione dei Dati Personali, al fine di garantire una concreta ed efficace gestione della violazione avvenuta e dei rischi connessi.

Tutti i soggetti destinatari del presente documento, ove nello svolgimento delle proprie mansioni rileveranno l'accadimento di una Violazione dei Dati Personali e/o matureranno il ragionevole sospetto circa l'accadimento di una Violazione dei Dati Personali, sono tenuti ad agire in conformità di quanto di seguito indicato.

2. Rilevazione di una Violazione dei Dati Personali

La Società potrà venire a conoscenza di una Violazione dei Dati Personali in via diretta o in via indiretta, tramite l'ausilio dei Responsabili del Trattamento, i quali, per obbligo di legge (art. 33, paragrafo 2, del Regolamento), devono informare tempestivamente il Titolare del Trattamento, ove vengano a conoscenza di una Violazione dei Dati Personali di titolarità della Società.

Ciascun amministratore, dirigente, dipendente, collaboratore e stagista, non appena venga a conoscenza di una concreta o sospetta Violazione dei Dati Personali è tenuto a comunicare tale accadimento all'Amministratore di sistema, immediatamente e, comunque, nel più breve tempo possibile (ad esempio, un dipendente subisce il furto del telefono cellulare aziendale oppure un dirigente rileva la cancellazione totale o parziale di un database contenente informazioni sui fornitori della Società).

In particolare, la comunicazione andrà effettuata tempestivamente e per iscritto all'indirizzo e-mail dell'Amministratore di Sistema. Ove possibile la comunicazione scritta dovrà essere preceduta da una telefonata all'Amministratore di Sistema.

Sarà cura dell'Amministratore di Sistema – incaricato di monitorare e gestire tutte le comunicazioni interne relativamente a sospette e/o verificatesi Violazioni dei dati personali – informare immediatamente il DPO.

Nel caso in cui il Data Breach sia solamente sospetto:
• ai fini del rispetto delle prescrizioni poste dal Regolamento in capo alla Società (si veda il successivo paragrafo 4), la Società deve raggiungere nel più breve tempo possibile un ragionevole grado di certezza circa l'avvenuta verificazione di una Violazione dei Dati Personali;
• a tal fine, il DPO e l'Amministratore di Sistema avviano immediatamente una fase d'indagine, volta a verificare se il Data Breach si sia effettivamente verificato. L'indagine è tesa a verificare con un ragionevole grado di certezza se la Violazione dei Dati Personali è avvenuta: un'investigazione più dettagliata deve avere luogo successivamente (a titolo esemplificativo, l'indagine volta ad accertare il numero di

Interessati colpiti dovrà essere effettuata solamente una volta raggiunto il predetto ragionevole grado di certezza).

3. Registro dei Data Breach

3.1. Compilazione e tenuta del Registro dei Data Breach

Ai sensi dell'art. 33, paragrafo 5, del Regolamento la Società, in qualità di Titolare del Trattamento, documenta qualsiasi Violazione dei Dati Personali per mezzo del registro dei Data Breach, tenuto dalla Società.

Una volta che è stato raggiunto un ragionevole grado di certezza in merito ad una Violazione dei Dati Personali, dovrà essere completato il registro dei Data Breach con tempestività.

Il soggetto incaricato e responsabile della compilazione del registro dei Data Breach è l'Amministratore di sistema della Società. L'Amministratore di sistema deve avviare e portare a termine tutta la procedura relativa alla compilazione del registro dei Data Breach, come indicato nel presente documento.

L'Amministratore di sistema, ove necessario, nell'operare nel rispetto delle presenti linee guida, potrà rivolgersi al DPO, al fine di ottenere supporto e maggiori indicazioni per il corretto svolgimento dell'incarico assegnatogli.

3.2. Contenuto

Il registro dei Data Breach della Società deve contenere le seguenti voci:

1. **Evento**, ovvero la tipologia di incidente verificatosi;
2. **Data**, ovvero la data in cui è avvenuto l'incedente e/o si è scoperto il Data Breach;
3. **Tipologia di dati**, ovvero la tipologia di dati coinvolti;
4. **Trattamento**, ovvero la tipologia di trattamento effettuato sui dati coinvolti;
5. **Soggetti intervenuti**, ovvero le persone che sono state coinvolte nell'attività di accertamento e *recovery*;
6. **Notifica all'Autorità di Controllo**, ovvero se è stato necessario notificare all'Autorità di Controllo l'incidente;
7. **Comunicazione agli Interessati**, ovvero se è stato necessario comunicare agli Interessati l'incidente;
8. **Descrizione**, ovvero un breve resoconto di quanto successo, come si è intervenuti e a quali risultati ha portato l'intervento;
9. **Note**, ovvero l'indicazione di eventuali note aggiuntive che possono essere rilevanti per il caso di specie.

4. Azioni da intraprendere e valutazioni sul Data Breach da effettuarsi

Una volta effettuata la (parziale) compilazione del registro con le informazioni a disposizione dell'Amministratore di sistema, quest'ultimo dovrà rivolgersi nuovamente al DPO illustrando quanto effettivamente riportato nel registro dei Data Breach, nonché le concrete azioni di messa in sicurezza che sono state intraprese.

In particolare, se esistono azioni che possano limitare i danni che la Violazione dei Dati Personali potrebbe causare agli Interessati (i.e. riparazione fisica di strumentazione; l'utilizzo dei file di back up per recuperare dati persi o danneggiati; isolamento/chiusura di un settore compromesso della rete; modifica di codici di accesso; ecc.), l'Amministratore di sistema è tenuto ad eseguirle immediatamente e senza ingiustificato ritardo (nonché a riportarle nell'apposito Registro dei Data Breach).

Il DPO, eventualmente coadiuvato dai vertici societari, provvederà ulteriormente ad analizzare quanto accaduto, a valutare le azioni intraprese da parte

dell'Amministratore di sistema al fine di valutare se quanto dallo stesso messo in atto sia consono e proporzionato alla Violazione dei Dati Personali rilevata.
Il DPO, infine, supportato anche dall'Amministratore di sistema e dai vertici societari, dovrà rendere il suo parere circa Violazione dei Dati Personali e, in particolare, concludere se questa possa ritenersi conclusa senza necessità di notifica ex artt. 33 e 34 Regolamento o se, al contrario, si debba procedere con la notifica all'Autorità di Controllo competente e/o la comunicazione agli Interessati.
In ogni caso, ove l'intervenuta Violazione dei Dati Personali ha avuto riguardo dati personali trattati dalla Società in veste di Responsabile del Trattamento, la Società dovrà procedere con la comunicazione della Violazione dei Dati Personali al Titolare del Trattamento, nel rispetto di quanto previsto dall'art. 33, paragrafo 2, del Regolamento e delle modalità e linee guida indicate nel successivo paragrafo 5.2.
In base alle determinazioni assunte, sarà compito dell'Amministratore di sistema riportare i dettagli delle decisioni prese e delle azioni intraprese all'interno del registro dei Data Breach.

5. Comunicazione all'esterno del Data Breach verificatosi

In caso di determinate Violazioni dei Dati Personali, il GDPR impone degli adempimenti di notifica e di comunicazione all'esterno, sia in capo al Titolare del Trattamento che in capo al Responsabile del Trattamento (si vedano gli artt. 33-34 del Regolamento).

5.1. Procedura da adottare quando la Società agisce in qualità di Titolare del Trattamento

5.1.1. Notifica all'Autorità di Controllo

Il Regolamento all'art. 33, paragrafo 1, impone al Titolare del Trattamento l'obbligo di notifica all'Autorità di Controllo ove la Violazione dei Dati Personali degli Interessati presenti un rischio per i diritti e le libertà delle persone fisiche.
A titolo esemplificativo, la Società potrebbe ritenere – a seguito di un'analisi specifica del Data Breach verificatosi, delle circostanze dello stesso e della tipologia e della gravità dei rischi che esso pone in capo agli Interessati – che potrebbe concretizzarsi tale rischio:

- nel momento in cui si realizzi una perdita di controllo, da parte dell'Interessato, relativamente ai propri Dati Personali;
- nel caso in cui si realizzi una limitazione relativa alla possibilità di esercitare un determinato diritto;
- qualora si possa verificare una possibile discriminazione dell'Interessato;
- nel caso in cui l'Interessato possa subire un furto di identità, una perdita economica, danni alla reputazione oppure uno svantaggio sociale ed economico per l'individuo possa verificarsi;
- nel caso in cui si sia verificata la perdita di confidenzialità di dati protetti da segreto professionale.

In particolare, quando agisce in qualità di Titolare, la Società deve notificare la Violazione dei Dati Personali all'Autorità di Controllo competente senza ingiustificato ritardo e, ove 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 la notifica all'Autorità di Controllo non sia effettuata entro 72 ore, la Società deve corredare la notifica dei motivi del ritardo. È compito del DPO, con il supporto

dell'Amministratore di Sistema, curare la redazione dell'apposito testo, da trasmettere all'Autorità di Controllo, per descrivere i motivi
del ritardo.
La notifica all'Autorità di Controllo deve almeno:

- 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;
- comunicare il nome e i dati di contatto del DPO o di altro punto di contatto presso cui ottenere più informazioni;
- 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 anche, se del caso, per attenuarne i possibili effetti negativi.

Ove il DPO, a conclusione della procedura indicata nel precedente paragrafo 4, fornisca parere circa la necessità di procedere con la notifica al Garante, l'Amministratore di sistema dovrà procedere con l'invio della notifica al Garante tramite l'apposita procedura telematica[1], entro 72 ore dalla scoperta della violazione e comunque con tempestività e senza ingiustificato ritardo.
Prima di procedere con l'invio della notifica, l'Amministratore dovrà compilare l'apposito modello facsimile, reso disponibile dal Garante[3], per poter mostrare, in anteprima, al DPO i contenuti che saranno comunicati al Garante. Il modello facsimile, una volta compilato, dovrà essere quindi preventivamente inviato al DPO al fine di ottenere un suo parere. Successivamente, una volta ottenuto il parere positivo del DPO, l'Amministratore di sistema procederà con l'invio della notifica al Garante, seguendo le indicazioni presenti sul sito.
Ai sensi dell'art. 33, paragrafo 4, del Regolamento, "*Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo*".
In particolare, in assenza di un quadro completo della Violazione dei Dati Personali intercorsa, con riserva di effettuare una successiva notifica integrativa, l'Amministratore di Sistema dovrà indicare che si sta procedendo con una notifica "*preliminare*".
Una volta trasmessa la notifica preliminare, sarà cura dell'Amministratore di Sistema, coadiuvato dal DPO, effettuare le ulteriori indagini necessarie al rinvenimento delle ulteriori informazioni richieste dal Regolamento al fine di fornirle all'Autorità di Controllo competente senza ulteriore ingiustificato ritardo (per il tramite della notifica cosiddetta "*integrativa*"). Una volta rinvenute le predette informazioni, l'Amministratore di Sistema dovrà procedere con la compilazione del modello facsimile predetto, segnalando che si tratta di una notifica "*integrativa*" nonché inserendo il numero del fascicolo ed il relativo PIN, assegnati alla precedente notifica, ed inviarlo al DPO per ottenere il suo parere. Una volta ottenuto il parere del DPO, sarà cura dell'Amministratore di sistema procedere con la trasmissione della notifica integrativa al Garante.

5.1.2. Comunicazione agli Interessati

L'art. 34 del Regolamento prevede l'obbligo di comunicazione di una Violazione dei Dati Personali all'Interessato, quando la Violazione dei Dati Personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.
Tale comunicazione non è richiesta se:

(i) il Titolare 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;
(ii) ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli Interessati;
(iii) detta comunicazione richiederebbe sforzi sproporzionati (in tal caso, si deve procedere invece a una comunicazione pubblica o a una misura simile, tramite la quale gli Interessati sono informati con analoga efficacia).
La Società, nell'effettuare la comunicazione, dovrà procedere privilegiando modalità di comunicazione diretta con gli Interessati (a titolo esemplificativo, ma non esaustivo: l'invio di una e-mail, l'invio di un SMS…). Il messaggio dovrà essere comunicato in maniera evidente e trasparente e con modalità facilmente comprensibili per gli Interessati. Altresì, sarà possibile effettuare una comunicazione pubblica, purché mantenga lo stesso grado di efficacia conoscitiva del contatto diretto con l'interessato.
La comunicazione della Violazione dei Dati Personali agli Interessati dovrà:

- contenere una descrizione della natura della Violazione dei Dati Personali e delle possibili conseguenze della stessa;
- fornire agli Interessati indicazioni specifiche sulle misure eventualmente da loro adottabili per proteggersi da eventuali conseguenze negative della Violazione dei Dati Personali (a titolo esemplificativo, la comunicazione potrà raccomandare agli Interessati di non utilizzare più le credenziali compromesse e/o di modificare la password utilizzata per l'accesso a qualsiasi altro servizio online qualora coincidente o simile a quella oggetto di Data Breach).

Conseguentemente, ove il DPO, a conclusione della procedura indicata nel precedente paragrafo 4, fornisca parere circa la necessità di procedere con la comunicazione agli Interessati, salva diversa decisione dei vertici aziendali, l'Amministratore di sistema, il soggetto preposto all'adempimento del presente obbligo di comunicazione agli Interessati, predisporrà la comunicazione agli Interessati. La comunicazione agli Interessati, una volta predisposta, dovrà essere preventivamente oggetto di parere del DPO, il quale dovrà esprimersi altresì circa le modalità decise dalla Società per l'inoltro della comunicazione.
Altresì, la Società dovrà procedere alla comunicazione del Data Breach agli Interessati nel caso in cui l'Autorità di Controllo ingiunga alla Società di procedere in tal senso ai sensi dell'art. 58, paragrafo 2, lett. e) del Regolamento (tra i poteri correttivi delle Autorità di Controllo infatti rientra il seguente:
"*ingiungere al titolare del trattamento di comunicare all'interessato una violazione dei dati personali*"). In tal caso, l'Amministratore di sistema oltre che rispettare le linee guida qui riportate dovrà, se del caso, rispettare anche le indicazioni date dall'Autorità di Controllo.

5.2. Procedura da adottare quando la Società agisce in qualità di Responsabile del Trattamento

Nel caso in cui la Società operi in qualità di Responsabile del Trattamento in relazione ad una Violazione dei Dati Personali verificatasi, la Società deve informare il Titolare senza ingiustificato ritardo dopo esserne venuto a conoscenza.
Nello specifico, una volta accertato dall'Amministratore di Sistema che la Violazione dei Dati Personali sia riferibile a Dati Personali che la Società tratta in qualità di

Responsabile del Trattamento, per conto di un Titolare del Trattamento, il DPO dovrà procedere all'esame della nomina a Responsabile del Trattamento per poter procedere con la notifica, come di seguito indicato:

• la procedura prevista nella nomina: la Società deve seguire le istruzioni contenute nella nomina a Responsabile del Trattamento e/o comunque condivise con la Società da parte del Titolare del trattamento (per quanto riguarda le modalità e le tempistiche della notifica della Violazione dei Dati Personali) come procedura specifica per notificare il Data Breach al Titolare del Trattamento (utilizzando, a titolo esemplificativo, eventuali moduli/canali di contatto e/o predisposti dal Titolare ed allegati all'atto di nomina). Il DPO può supportare la Società nella verifica delle istruzioni ricevute;

• la procedura generale della Società in qualità di Responsabile del Trattamento: se la nomina a Responsabile del Trattamento non stabilisce alcuna specifica procedura, la notifica dovrà in ogni

caso almeno includere i seguenti elementi:

- descrizione della 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;
- comunicazione del nome e dei dati di contatto del DPO e dell'Amministratore di Sistema presso cui ottenere più informazioni;
- descrizione delle probabili conseguenze della Violazione dei Dati Personali;
- descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla Violazione dei Dati Personali e anche, se del caso, per attenuarne i possibili effetti negativi.

In particolare, la Società deve individuare nella nomina a Responsabile del Trattamento e/o nel contratto i contatti ufficiali del Titolare del Trattamento, tramite i quali, senza ingiustificato ritardo, dovrà essere notificata la Violazione dei Dati Personali utilizzando il modulo per la notifica del Data Breach al Titolare del Trattamento di cui all'Allegato 1.

L'Amministratore di Sistema è il soggetto deputato alla compilazione del modulo di notifica predetto. Il modulo, una volta compilato, dovrà essere oggetto di parere da parte del DPO.

Successivamente dovrà procedersi alla comunicazione al Titolare tramite invio al Titolare del Trattamento del modulo via PEC (ove non sia disponibile l'indirizzo PEC del Titolare del Trattamento si dovrà procedere via lettera raccomandata A/R anticipata via e-mail ordinaria).

L'Amministratore di Sistema e il DPO saranno responsabili per qualsiasi domanda e/o richiesta ulteriore da parte del Titolare del Trattamento.

Allegato 1 – Modulo di notifica di una Violazione dei Dati Personali al Titolare del Trattamento

Oggetto: Notifica di una violazione dei dati personali ai sensi dell'art 33 par. 2 del GDPR
Spettabile inserire denominazione del Titolare del Trattamento, la scrivente [inserire denominazione della scrivente], con sede legale in [inserire indirizzo], C.F./P.IVA/Registro Imprese di [inserire città, se applicabile]: [...], in persona del suo legale rappresentante Dott. ... (di seguito, la "Società"), notifica di seguito l'avvenuta violazione di dati personali dalla Società trattati per Vostro conto – ai sensi del contratto di servizi/collaborazione/partnership stipulato il ... e dell'atto di nomina a responsabile del trattamento sottoscritto tra le parti il ... – i cui tempi e modalità sono di seguito descritti in dettaglio.

1. Dati di contatto

Nome e Cognome della persona fisica addetta alla comunicazione	Inserire
Funzione rivestita, ruolo, mansioni ed eventuali incarichi di trattamento nell'organizzazione della Società	Amministratore di sistema
Recapito e-mail e/o telefonico per eventuali comunicazioni	Inserire
Indirizzo e-mail del DPO della Società	Inserire

2. Dettagli della Violazione dei Dati Personali

Sono stati coinvolti Dati Personali e informazioni riconducibili a persone identificate o identificabili?	☐Si ☐No ☐Forse
Quali categorie di registrazioni di Dati Personali sono state coinvolte dalla Violazione dei Dati Personali?	Inserire le categorie di registrazioni di Dati Personali coinvolte (ad es. numeri di telefono, e-mail, dati idonei a rivelare lo stato di salute ecc.)
Quante categorie di registrazioni di Dati Personali sono state coinvolte dalla Violazione dei Dati Personali?	Inserire il numero approssimativo di categorie di registrazioni di Dati Personali coinvolte ☐ Sono stati coinvolti un numero (ancora) sconosciuto di categorie di registrazioni di Dati Personali
Quali Interessati sono stati coinvolti dalla Violazione dei Dati Personali?	Inserire le categorie di Interessati (ad es. clienti, dipendenti ecc.)
Quanti Interessati sono stati coinvolti dalla Violazione dei Dati Personali?	Inserire il numero approssimativo di Interessati coinvolti dalla Violazione dei Dati Personali ☐ Sono stati coinvolti un numero (ancora) sconosciuto di Interessati
Quali sono le possibili conseguenze per gli Interessati coinvolti derivanti dalla Violazione dei Dati Personali?	Ad esempio: ☐ furto d'identità ☐ perdite finanziarie ☐ pregiudizio alla reputazione ☐danno economico o sociale ☐decifratura non autorizzata della pseudonimizzazione ☐discriminazione degli Interessati ☐altro: specificare
Spiegare e descrivere dettagliatamente (*i*) cosa è accaduto (ad es. alterazione, cancellazione, copia ecc. dei Dati Personali); (*ii*) la causa che ha scatenato o ha dato vita alla Violazione; (*iii*) la natura (accidentale oppure illecita) della Violazione Si prega di includere dettagli in merito, come ad esempio (*a*) se esistono logs file in grado di fornire informazioni in merito alla cronologia degli eventi che hanno dato vita alla Violazione; (*b*) informazioni sulla confidenzialità, l'integrità e disponibilità dei Dati Personali; (*c*) le circostanze che hanno connotato la Violazione	
Dove è avvenuta la Violazione dei Dati Personali?	
La Violazione è avvenuta su sistemi, applicazioni e/o dispositivi della Società o di terze parti? Specificare il nome dei sistemi, delle applicazioni e/o dei dispositivi su cui è avvenuta la Violazione.	
Data e ora in cui la Violazione dei Dati Personali è cominciata	Inserire data e ora (oppure inserire "Tra il ___ e il ___") ☐ Data e ora in cui ha avuto inizio la Violazione dei Dati Personali non sono conosciute
Data e ora in cui la Violazione dei Dati Personali è terminata	Inserire data e ora ☐ La Violazione dei Dati Personali non è ancora terminata

3. Misure adottate dalla Società o delle quali la Società propone l'attuazione per porre rimedio alla Violazione dei Dati Personali e anche, se del caso, per attenuarne i possibili effetti negativi

La Società ha adottato delle misure per porre rimedio alla Violazione e/o per attenuarne i possibili effetti negativi?	☐No ☐Si: specificare
Indicare eventuali ulteriori soggetti (ad es. autorità di uno Stato membro) cui la Violazione è stata comunicata/notificata	

Stiamo svolgendo tutte le più opportune ricerche ed analisi al fine di potervi fornire, nel più breve tempo possibile, eventuali ulteriori dettagli a completamento del quadro informativo, anche per permettervi di operare le più opportune valutazioni ai sensi dell'art. 33 GDPR.