Manuale
procedure privacy

Digital Bros S.p.A.

Via Tortona, 37 – 20144 Milano, Italia
Partita IVA e codice fiscale 09554160151
Capitale sociale: Euro 6.024.334,80 di cui Euro 5.706.014,80 sottoscritto
Reg. Soc. Trib di Milano 290680-Vol. 7394 C.C.I.A.A. 1302132

La relazione è disponibile all'indirizzo www.digitalbros.com
nella sezione Privacy & Cookie Policy

GLOSSARIO

PERSONA FISICA: Si intende ogni singolo individuo;

PERSONE GIURIDICHE: Si intendono società, associazioni, enti o cooperative dotate di personalità giuridica;

DATI PERSONALI:

- **DATI IDENTIFICATIVI:** Si intendono i dati attraverso i quali è possibile ottenere l'identificazione diretta dell'interessato (Nome, Cognome, Codice Fiscale, Codice Cliente, etc.)
- **DATI PARTICOLARI**: Si intendono i dati che rivelano l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale nonché i dati che rivelano lo stato di salute o l'orientamento sessuale;
- **DATI GIUDIZIARI**: Si intendono i dati che rivelano provvedimenti giudiziari a carico della persona, in materia di: casellario giudiziale, anagrafe delle sanzioni amministrative o la qualità di imputato o indagato.

FIGURE IN AMBITO PRIVACY:

- **TITOLARE DEL TRATTAMENTO:** è 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.
    - Nel nostro caso è DIGITAL BROS S.P.A.
- **RESPONSABILE DEL TRATTAMENTO**: è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.
    - Nel nostro caso possono essere Consulenti, Fornitori di beni e servizi identificati nel registro delle terze parti.
- **DPO/RPD**: o ***Data Protection Officer***: è il "responsabile della protezione dei dati" che assiste il titolare del trattamento o il responsabile nel monitoraggio della compliance con la normativa applicabile in materia di protezione dei dati personali.
    - Nel nostro caso è l'Avv. Veronica Devetag Chalaupka (dpo@digitalbros.com)
- **PRIVACY OWNER:** è colui che garantisce l'applicazione delle misure di sicurezza e delle regole per la gestione e la protezione dei dati le cui finalità ricadono sotto la sua responsabilità.

- Nel nostro caso sono tutti i responsabili di ufficio, nonché dirigenti.

- **RESPONSABILE PRIVACY**: definisce i processi e le procedure aziendali a garanzia di un corretto trattamento dei dati personali e cura la predisposizione della documentazione necessaria agli adempimenti in materia Privacy.
  - Nel nostro caso è il General Counsel, Avv. Dario Treves.
- **INCARICATO:** è colui che, autorizzato ai sensi di una nomina scritta, tratta i dati secondo policy, procedure e regole vigenti e su indicazioni ricevute dal Titolare.
  - Nel nostro caso sono tutti i dipendenti.
- **INTERESSATO**: è la persona fisica che può essere identificata, direttamente o indirettamente.
  - Nel nostro caso Dipendenti, clienti, fornitori.
- **DPIA** / "*Data Protection Impact Assessment*": analisi di impatto più approfondita al fine di individuare le misure di contenimento e protezione dei dati degli interessati.

*****

GESTIONE DEI DATA BREACH

PRINCIPI GENERALI

La violazione di dati è un particolare tipo di incidente di sicurezza, per effetto del quale, il titolare non è in grado di garantire il rispetto dei "Principi applicabili al trattamento di dati personali" prescritti dal GDPR.

Una violazione di dati personali deriva da situazioni in cui i dati personali, in formato elettronico o fisico, sono soggetti a:

- violazione di Confidenzialità: quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale.
- violazione di Integrità: quando si verifica un'alterazione (modifica) di dati personali non autorizzata o accidentale.
- violazione di Disponibilità: quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.

L'art. 33 del GDPR sancisce che, in caso di violazione dei dati personali, il Titolare del trattamento deve notificare la violazione 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 degli interessati (persone fisiche). inoltre, il

Titolare deve documentare ogni evento che potenzialmente sia configurabile come Data Breach, avendo anche a riferimento le indicazioni contenute nelle Linee Guida" rilasciate dal gruppo "Article 29 Data Protection Working Party" - WP29[1] (paragrafo II capoverso 2[2]), che prevedono eccezioni all'obbligo di notifica al fine di consentire all'Autorità stessa di verificare il rispetto complessivo della normativa.

Nel caso di rischio elevato per i diritti e le libertà degli individui, il Titolare del trattamento deve darne comunicazione anche agli interessati (art. 34).

Digital Bros S.p.A. deve quindi notificare all'Autorità eventuali violazioni dei dati personali (a seguito di attacchi informatici, accessi abusivi, incidenti o calamità naturali, come ad esempio incendi od alluvioni) che possano "mettere a rischio" le libertà e i diritti dei soggetti interessati.

Ne discende che le generali attività di Rilevamento, Valutazione, Notifica e Monitoraggio dell'incidente, devono essere documentate, dettagliate, tracciabili, replicabili e non modificabili in caso di verifica da parte del Garante.

È importante che sia dimostrabile il momento della scoperta dell'incidente (momento in cui il titolare diviene consapevole e ha avuto un ragionevole grado di certezza dell'avvenuta violazione), poiché da quel momento decorrono le 72 ore per la notifica.

Le Linee Guida del WP29 chiariscono che l'individuazione del momento a partire dal quale, un titolare può essere considerato "consapevole" di una particolare violazione dipenderà dalle circostanze della specifica violazione. In caso di violazioni dei dati personali che potrebbero comportare un rischio per i diritti e le libertà degli interessati Digital Bros S.p.A., quindi dovrà:

- notificare entro 72 ore la violazione dei dati personali all'Autorità; e
- comunicare, ove applicabile e senza indebito ritardo, a tutti gli interessati coinvolti, l'avvenuta violazione (questa condizione sussiste esclusivamente nel caso in cui la violazione dei dati possa comportare un rischio Elevato per i diritti e libertà dei soggetti coinvolti).

Nel caso in cui la notifica all'Autorità non venga effettuata entro 72 ore, il titolare dovrà fornire le motivazioni del ritardo (ad esempio problemi nella raccolta di tutte le informazioni necessarie per la notifica).

Laddove non sia possibile fornire tutte le informazioni richieste al momento della notifica, dovranno essere integrate non appena disponibili.

[1] Organismo consultivo e indipendente, composto da un rappresentante per ciascuna delle Autorità di protezione dei dati personali designate da ogni Stato membro, dal GEPD (Garante europeo della protezione dei dati), nonché da un rappresentante della Commissione Europea. Fra i compiti più rilevanti tra quelli disciplinati compare formulare di propria iniziativa raccomandazioni su qualsiasi questione riguardi la protezione dei dati personali nella Comunità Europea.
[2] Guidelines on Personal data breach notification under Regulation 2016/679 – adottate il 6 febbraio 2018

GESTIONE DEI DATA BREACH

Il processo di gestione dei Data Breach previsto da Digital Bros S.p.A. è composto da quattro fasi principali, illustrate nei seguenti paragrafi:

a. **Rilevamento**
b. **Valutazione**
c. **Notifica**
d. **Monitoraggio**

RILEVAMENTO

Le principali modalità di rilevazione che possono portare all'identificazione di una violazione possono consistere in:

- segnalazioni verso il Responsabile Sistemi Informatici, per temi inerenti alla sicurezza logica (come, ad esempio, l'individuazione di una violazione tramite strumenti di analisi e/o attività di verifica, controllo e monitoraggio dell'infrastruttura IT);
- segnalazioni verso il Responsabile Sistemi fisici per temi inerenti la sicurezza fisica / degli archivi fisici (come ad esempio l'individuazione di un incidente fisico tramite le attività di verifica e controllo).

Le segnalazioni possono provenire da diverse fonti:

- segnalazioni da parte di personale dipendente o di altro personale (ad esempio consulenti o soggetti autonomi) che lavora per Digital Bros S.p.A.;
- segnalazioni provenienti da soggetti terzi quali ad esempio clienti, fornitori altri soggetti che non hanno rapporti diretti con Digital Bros S.p.A., ivi incluse le segnalazioni pervenute direttamente dall'Autorità o da altri organismi pubblici (Polizia Postale, etc.,);
- segnalazioni ricevute dai soggetti nominati Responsabili Esterni del Trattamento dei dati personali.

Tutti i dipendenti di Digital Bros S.p.A. devono essere consapevoli dell'importanza di prestare attenzione a ciò che potrebbe costituire un Data Breach, alle sue potenziali minacce e come segnalare tempestivamente l'evento ai soggetti indicati, i quali provvederanno ad avvisare immediatamente il Responsabile Privacy ed il DPO.

SEGNALAZIONE VERSO FIGURE COMPETENTI

i. Segnalazione da parte di un dipendente

Qualora un dipendente rilevi un incidente / violazione della sicurezza logica (es. *cyber attack*, furto di un laptop, ecc.) o fisica (es. l'incendio o l'allagamento di un edificio contenete documentazione) che comporti anche accidentalmente la distruzione, la perdita, la modifica non autorizzata, la rivelazione non autorizzata, l'accesso non autorizzato ai dati personali trasmessi, memorizzati o comunque trattati, è necessario che quanto rilevato venga segnalato prontamente al **Responsabile Sistemi Informatici** (per temi inerenti la sicurezza logica) **o Responsabile Sistemi fisici** (per temi inerenti la sicurezza fisica / degli archivi fisici).

Qualora invece un soggetto autonomo, come ad esempio un consulente operante per Digital Bros S.p.A., rilevi una violazione della sicurezza dei dati personali, dovrà prontamente comunicarlo al proprio referente interno, che provvederà ad inoltrare la relativa segnalazione seguendo la procedura sopradescritta.

ii. Segnalazione da parte di un soggetto terzo

Qualora il Data Breach, rilevato da un soggetto terzo, quale ad esempio un cliente, fosse segnalato tramite un qualsiasi canale di contatto di Digital Bros S.p.A. (es. Telefono, mail, ecc.), il dipendente che riceve la comunicazione dovrà prontamente comunicarlo e segnalarlo seguendo la procedura sopra descritta (paragrafo i. Segnalazione da parte di un dipendente).

iii. Segnalazione da parte di un Responsabile Esterno del Trattamento

Il Responsabile Esterno deve comunicare al suo referente contrattuale (figura che in azienda detiene i rapporti col Responsabile stesso) ogni violazione della sicurezza che comporti anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai Dati Personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura, entro un massimo di 24 ore dal rilevamento dell'evento; in qualità di dipendente, il referente che riceve la comunicazione dovrà prontamente comunicarlo e segnalarlo seguendo la procedura sopradescritta (paragrafo .i. Segnalazione da parte di un dipendente).

Il Responsabile Esterno, a seguito della segnalazione, supporta il **Responsabile Privacy** nel processo di valutazione tramite la raccolta di tutte le informazioni necessarie per permettere, in modo completo e tempestivo l'eventuale notifica della violazione all'Autorità e, ove necessario, la comunicazione agli interessati di quanto accaduto.

Il Responsabile Esterno del Trattamento è tenuto a rispondere tempestivamente ad ogni richiesta di informazioni pervenuta da parte del titolare.

RILEVAZIONE DEGLI INCIDENTI NELL'AMBITO DELLE ATTIVITÀ DI MONITORAGGIO

Al fine di poter rilevare una violazione di dati personali in modo tempestivo tenuto conto dei requisiti normativi applicabili, Digital Bros S.p.A. ha previsto l'implementazione di misure organizzative e tecniche per l'individuazione e la prevenzione di eventuali incidenti, nel rispetto del principio di proporzionalità.

Il Responsabile Sistemi Informatici fornisce misure organizzative e tecniche (ad esempio procedure, strumenti per la prevenzione e il rilevamento delle intrusioni, ecc.) per prevenire, rilevare e segnalare eventuali incidenti rientranti nella sfera IT.

Il o Responsabile Sistemi fisici tramite gli strumenti messi a protezione degli archivi fisici gestiti e al perimetro della sicurezza fisica di competenza, potrebbero rilevare il verificarsi di un incidente, con un potenziale impatto sui dati personali: in questo caso provvederà a segnalare il potenziale Data Breach al Responsabile Privacy che, dopo opportune valutazioni, avvierà il processo di Data Breach, avvalendosi delle figure competenti.

AVVIO DEL PROCESSO DI GESTIONE DATA BREACH

Sulla base delle segnalazioni ricevute e/o di quelle rilevate da parte del Responsabile Sistemi Informatici e del Responsabile dei sistemi fisici secondo le modalità di cui al paragrafo i, il Responsabile Privacy effettuerà una prima valutazione di massima, con il supporto del DPO, per determinare se l'evento in questione possa essere valutato come potenziale Data Breach.

A tal fine, il Responsabile Privacy potrà inviare eventuali richieste di approfondimento ai diversi Privacy Owner delle aree coinvolte e, se necessario, al Responsabile Sistemi Informatici e al o Responsabile Sistemi fisici.

I Privacy Owner delle aree coinvolte raccolgono le informazioni necessarie per la valutazione dell'evento richieste dal Responsabile Privacy avvalendosi, se necessario, del supporto del Responsabile Sistemi Informatici e del o Responsabile Sistemi fisici.

Per poter analizzare il possibile evento di Data Breach dovrebbero essere acquisite le seguenti informazioni minime, all'interno del *Modulo Raccolta Informazioni*:

- *Data e ora in cui si è verificato*
- *Data e ora in cui è stato rilevato*
- *Chi / cosa lo ha segnalato*
- *Descrizione della natura della violazione*
- *Numero approssimativo e categoria di interessati coinvolti*
- *Numero approssimativo e categoria dei dati personali violati*

- *Dettagli del/i sistema/i IT interessato*
- *Archivi fisici o dispositivi rimovibili coinvolti*
- *Misure di sicurezza in atto*
- *Materiale a supporto della rilevazione, come ad esempio messaggi di errore, LOG, ecc.*
- *Misure adottate o di cui si propone l'adozione per ridurre l'impatto o porre rimedio al Data Breach.*

Al fine di permettere un'analisi completa del Data Breach si dovrà prestare la massima attenzione a che le informazioni siano sempre aggiornate, raccolte con meticolosità e condivise tempestivamente con tutti gli attori coinvolti nella gestione dell'evento facendo in modo che sia sempre disponibile un quadro informativo il più possibile completo e aggiornato.

Nel caso in cui, a seguito della valutazione di massima, l'evento sia valutato come potenziale Data Breach, il Responsabile Privacy provvede a convocare il Comitato per la gestione dei Data Breach (così come descritto al paragrafo successivo). In ogni caso, sarà compito del Comitato di Gestione dei Data Breach analizzare le informazioni raccolte e valutare se procedere o meno ad effettuare la notifica all'Autorità e/o all'interessato.

IL COMITATO PER LA GESTIONE DEI DATA BREACH

Il Comitato per la gestione dei Data Breach ha come scopo la valutazione dell'evento rilevato e l'individuazione delle azioni da intraprendere nel caso si configuri come un Data Breach.

I principali compiti del Comitato per la gestione dei Data Breach sono:

- Analizzare l'evento;
- Valutare se debba essere classificato come una violazione dei dati personali;
- Valutare se è necessario procedere alla notifica all'Autorità;
- Valutare se è necessario comunicare agli interessati;
- Individuare le misure di mitigazione da implementare.

Il Comitato per la gestione dei Data Breach è costituito dalle seguenti funzioni:

- DPO
- Responsabile Privacy
- Responsabile Sistemi Informatici
- Responsabile dei sistemi fisici
- Amministratore di sistema
- Eventuali altri membri di cui viene valutata la partecipazione sulla base delle circostanze, come ad esempio:
    - Privacy Owner coinvolto nell'evento.

VALUTAZIONE

Il Comitato per la gestione dei Data Breach, sulla base delle informazioni ricevute, effettua una valutazione dell'evento, al fine di individuare la presenza ed il livello di rischio per i diritti e le libertà degli interessati.

Per valutare il livello di rischio è necessario considerare i seguenti aspetti:

- Tipo di informazioni / dati coinvolti (es. nome e cognome, domicilio o altri indirizzi di residenza, informazioni su età, sesso, indirizzi e-mail, numeri di telefono, numero di passaporto, patente di guida, informazioni personali sensibili, ecc.)
- Meccanismi di sicurezza in atto (es. controllo degli accessi, crittografia, ecc.)
- Interessati coinvolti dalla violazione (es. numero di soggetti interessati, nome, contatti, ecc.)
- Azioni da intraprendere o già in corso per mitigare le perdite e limitare l'impatto della violazione dei dati personali (es. blocco degli accessi a specifici sistemi, aggiornamenti dei sistemi, ecc.)
- Potenziali conseguenze negative, associate all'effettiva compromissione, per i soggetti interessati.

Il Considerando 88 del GDPR specifica che è necessario stabilire se i dati personali fossero o meno protetti con misure tecniche adeguate di protezione atte a limitare efficacemente il rischio di furto d'identità o altre forme di abuso.

FATTORI DA CONSIDERARE QUANDO SI VALUTA IL RISCHIO DELLA VIOLAZIONE

I considerando 75 e 76 del GDPR suggeriscono che, nella valutazione del rischio, si dovrebbe prendere in considerazione sia la gravità/impatto che lo stesso comporterebbe per i diritti e le libertà degli interessati, sia la probabilità che lo stesso avvenga.

Si fa presente inoltre che il rischio dovrà essere valutato oggettivamente.

Nel valutare il rischio che potrebbe derivare da una violazione, il titolare del trattamento dovrebbe considerare una combinazione della gravità dell'impatto potenziale sui diritti e le libertà delle persone fisiche e la probabilità che esse si verifichino. Chiaramente, laddove le conseguenze di una violazione sono più gravi, il rischio è più elevato e, analogamente, laddove la probabilità che ciò si verifichi sia maggiore, aumenta anche il rischio.

Per poter valutare adeguatamente il rischio associato al Data Breach in analisi, devono essere analizzati specifici fattori, ovvero:

Fattore da considerare	Ambito di valutazione
Il tipo di violazione	Definire il tipo violazione in termini di Confidenzialità, Integrità e Disponibilità. Ad esempio, una violazione della confidenzialità, in base alla quale le informazioni sono state divulgate a soggetti non autorizzati, può avere conseguenze diverse per un individuo rispetto ad una violazione in cui le informazioni di un individuo sono state perse e non sono più disponibili.
La natura, la tipologia e il volume dei dati personali	Identificare la natura (es. tipologia di dati personali), il livello di tipologia (es. dati che possano rilevare origini raziali di un individuo) e volume (in termini di quantità) di dati personali violati. Più tipologie di dati sono coinvolte, maggiore è il rischio potenziale per gli interessati. Inoltre devono essere presi in considerazione anche altri aspetti relativi ai dati trattati, come ad esempio: • È improbabile che la divulgazione del nome e dell'indirizzo di un individuo in circostanze ordinarie causi un danno sostanziale, tuttavia, se il nome e l'indirizzo di un genitore adottivo sono divulgati a un genitore naturale, le conseguenze potrebbero essere molto gravi sia per il genitore adottivo che per il bambino; • Un elenco di clienti che richiedono consegne regolari potrebbe non essere particolarmente sensibile, ma gli stessi dati inerenti a clienti che hanno richiesto che le loro consegne vengano interrotte durante le vacanze sarebbero informazioni utili ai criminali.
Facilità di identificazione delle persone	Rilevare la facilità con cui è possibile identificare un soggetto ovvero se le informazioni in questione possono permettere di individuare uno specifico individuo e con quanta precisione sia possibile farlo. Ad esempio la facilità con cui una soggetto malevolo può accedere a dati personali per identificare persone specifiche o abbinare i dati con altre informazioni per identificare gli individui. A seconda delle circostanze, l'identificazione potrebbe essere possibile direttamente dai

	dati personali violati senza alcuna ricerca specifica necessaria per scoprire l'identità dell'individuo, oppure potrebbe essere estremamente difficile abbinare i dati personali a un particolare individuo, ma potrebbe comunque essere possibile a determinate condizioni (es. conoscenza della chiave di decriptazione).
Gravità delle conseguenze per gli individui	Individuare le conseguenze per gli individui derivanti dalla violazione e la relativa gravità. A seconda della natura dei dati personali coinvolti in una violazione, ad esempio, categorie particolari di dati, il potenziale danno che potrebbe derivarne per gli individui potrebbe essere particolarmente grave, in particolare laddove la violazione possa comportare furto di identità o frode, danno fisico, disagio psicologico, umiliazione o danno alla reputazione. Se la violazione riguarda dati personali di individui vulnerabili (es. minori), gli stessi potrebbero essere esposti ad un maggior rischio di danno.
Caratteristiche speciali dell'individuo	Rilevare la presenza di individui con caratteristiche speciali, quali ad esempio minori o portatori di invalidità. Una violazione può influire sui dati personali relativi ai bambini o ad altre persone vulnerabili (es. disabili), di conseguenza questi soggetti potrebbero essere esposti a maggiori pericoli.
Caratteristiche particolari del Titolare del trattamento dei dati	Definire le caratteristiche del titolare del trattamento (es. clinica ospedaliera). A seguito di una violazione, la natura, il ruolo del titolare del trattamento e le sue attività, possono influire sul livello di rischio per le persone. Ad esempio, un'organizzazione medica elabora categorie speciali di dati personali, il che significa che se i dati personali delle persone vengono violati vi è una maggiore minaccia rispetto alla violazione di una mailing list di un giornale.
Numero di individui coinvolti	Definire il numero di individui coinvolti. Una violazione può riguardare solo uno o pochi individui o diverse migliaia, se non molti di più. Generalmente, maggiore è il numero di

	individui interessati, maggiore è l'impatto di una violazione. Tuttavia, una violazione può avere un impatto grave anche su un solo individuo, a seconda della natura dei dati personali e del contesto in cui sono stati violati i dati.
Misure di Sicurezza in essere a protezione dei dati	Identificare le misure di sicurezza in essere a protezione dei dati. Ad esempio i dati personali protetti tramite un livello appropriato di crittografia, senza la chiave di decrittazione, saranno incomprensibili a soggetti malevoli e/o soggetti senza l'autorizzazione ad accedere a tali dati. Altresì i dati personali protetti da pseudonimizzazione, attuata in modo tale da impedire che i dati personali possano essere attribuiti a un interessato specifico senza l'uso di ulteriori informazioni (che vengono conservate separatamente), possono anche ridurre la probabilità che gli individui vengano identificati in caso di violazione. Tuttavia, le sole tecniche di pseudonimizzazione non possono essere considerate come intelligibili.
Misure di Sicurezza da attuare per la protezione dei dati	Individuare le misure di sicurezza di cui ci si dovrà dotare ed adottare per proteggere i dati. Ad esempio nel caso in cui venisse scoperta una vulnerabilità di un sistema bisognerà prontamente provvedere al relativo aggiornamento (patch management).

Sulla base dell'analisi dei fattori sopra riportati, per ciascuna violazione bisogna valutare l'Impatto e la Probabilità relativi ai rischi per gli interessati. Per eseguire l'analisi dell'impatto di seguito sono riportati i possibili livelli di valutazione associati all'impatto stesso.

Impatto	**Descrizione dell'impatto**	**Valore**
Basso	Gli individui non saranno impattati dalla violazione o potrebbero essere impattati da alcuni superflui inconvenienti, che saranno in grado di superare senza alcun problema (es. tempo trascorso a reinserire informazioni, fastidi, irritazioni, ecc.)	1

Medio	Gli individui possono incontrare notevoli disagi, che saranno in grado di superare nonostante alcune difficoltà (es. paura, mancanza di comprensione, stress, disturbi fisici minori, ecc.)	2
Alto	Gli individui possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (es. appropriazione indebita di fondi, *blacklist* bancaria, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, aggravamento della salute, ecc.)	3
Molto alto	Gli individui possono incontrare conseguenze significative, o addirittura irreversibili, che non possono superare (difficoltà finanziarie come debito sostanziale o incapacità lavorativa, disturbi psicologici o fisici a lungo termine, morte, ecc.)	4

A seguito della valutazione dell'impatto del Data Breach, si deve valutare la probabilità che l'impatto individuato si verifichi, ovvero se la minaccia si possa realizzare o meno.

Probabilità	**Descrizione della probabilità**	**Valore**
Bassa	La minaccia / rischio non si può realizzare La minaccia/rischio non può verificarsi o è remota la possibilità che si realizzi	1
Media	È probabile che la minaccia / rischio si realizzi	2
Alta	La minaccia / rischio si verificherà sicuramente prima o poi	3
Molto alta	La minaccia si realizzerà con certezza nel prossimo futuro	4

Definiti impatto e probabilità e moltiplicandone il valore assegnato tramite la formula "IxP" (impatto X probabilità), si otterrà, il livello di classificazione da assegnare alla violazione. Di seguito viene riportato l'intervallo tramite cui è possibile assegnare una classificazione al Data Breach.

Classificazione	**Intervallo del rischio**	**Note per la Classificazione**
Rischio Trascurabile	Valore finale tra 1 e 3 compresi	Non viene rilevata alcuna forma di rischio per la sicurezza dei dati, 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.
Presenza di Rischio	Valore finale tra 4 e 11 compresi	Sono coinvolte nella violazione informazioni personali comuni (es. dati identificativi) Ci sarà un impatto potenziale sulla vita privata delle persone coinvolte (es. attività di spam)
Presenza di Rischio Elevato	Valore finale tra 12 e 16 compresi	Sono coinvolte nella violazione informazioni personali sensibili (es. dati sanitari, finanziari, giudiziari) Esiste un potenziale furto di identità Ci sarà un alto impatto sulla vita privata delle persone coinvolte a causa della compromissione di dati personali sensibili (es. attività di Spearphising)

Sulla base di quanto ottenuto dalla classificazione generale del rischio per gli interessati, si dovrà notificare il Data Breach all'Autorità Garante e, se necessario agli interessati. Di seguito vengono riportate le azioni da eseguire in base all'esito della classificazione.

Classificazione	**Azioni da compiere**
Rischio Trascurabile	Non c'è obbligo di Notifica all'Autorità La violazione viene registrata e documentata
Presenza di Rischio	C'è l'obbligo di Notifica all'Autorità La violazione viene registrata e documentata
Presenza di Rischio Elevato	C'è l'obbligo di Notifica all'Autorità Dopo aver avvertito e consultato l'Autorità, bisogna Comunicare agli Interessati la violazione La violazione viene registrata e documentata

Il Titolare, con il supporto del Comitato, provvede quindi a decidere se notificare o meno all'Autorità Garante la violazione e, ricorrendone le condizioni, anche agli Interessati: ad esempio, in caso di "rischio elevato per i diritti e le libertà" dell'Interessato, il Comitato dovrà valutare l'esigenza di procedere alla comunicazione dell'evento tenendo in considerazione anche i seguenti elementi:

- non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:
  - sono state messe in atto adeguate misure tecniche e organizzative per la protezione dei dati personali e tali misure sono 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;
  - sono state adottate misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
  - la comunicazione richiederebbe sforzi sproporzionati; in questo caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia. Possibili fattori da prendere in considerazione nella valutazione di questo caso potrebbero essere, tra gli altri, i costi, il tempo, la difficoltà nel fornire informazioni, etc.

La necessità di attenuare un rischio immediato di danno richiederebbe una tempestiva comunicazione agli interessati, mentre l'esigenza di attuare opportune misure per contrastare le violazioni di dati personali ripetute o analoghe può giustificare un ritardo nella comunicazione anche al fine di non ostacolare le attività di indagine.

NOTIFICA

Come descritto di seguito, il Comitato per la gestione dei Data Breach, a fronte del risultato della valutazione del rischio attribuito alla violazione dei dati personali, se necessario, avvierà il processo di Approvazione Interna e il processo di Notifica e Comunicazione Esterna.

A. APPROVAZIONE INTERNA

Di seguito vengono riportate le attività di reporting interno, che dovranno essere eseguite dal Comitato.

Il Comitato per la gestione dei Data Breach condivide con il Titolare lo stato di eventuali violazioni dei dati classificate come:

- Violazioni con Presenza di Rischio;
- Violazioni con Presenza di Rischio Elevato.

In tale contesto, il Comitato per la gestione dei Data Breach inoltre presenta al Titolare anche le misure di mitigazione già in essere e quelle previste per mitigare il rischio.

Sulla base della *Classificazione Rischio* viene redatto verbale delle determinazioni e annotata la decisione del Titolare; copia del verbale viene conservata a cura del DPO.

B. NOTIFICA E COMUNICAZIONE ESTERNA

In caso di approvazione il DPO, con il supporto del Coordinatore Privacy, gestisce sia la Notifica verso l'Autorità che la comunicazione ai soggetti Interessati.

Di seguito vengono riportate le tipologie di flussi comunicativi verso l'esterno:

- notifica all'Autorità;
- comunicazione agli interessati, ove applicabile.

Processo di notifica all'Autorità

Il DPO, sulla base di quanto deciso, notifica quanto accaduto all'Autorità, utilizzando i canali e/o i moduli previsti, eventualmente definiti dall'Autorità. Il Comitato per la gestione dei Data Breach supporta il DPO nel processo di notifica.

La notifica deve:

- 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 per fronteggiare la violazione dei dati personali, comprese, se del caso, le misure per mitigarne i possibili effetti negativi.

Stante l'importanza della tempestiva comunicazione all'Autorità qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contestualmente alla prima notifica, si procederà ad un inoltro delle ulteriori informazioni non appena disponibili. Le ragioni per cui il titolare potrebbe necessitare di maggior tempo per eseguire la notifica possono essere:

- complessità e numero dei sistemi (considerando anche quelli in uso presso terze parti), nonché dei dati che trattano;
- scoperta di più violazioni, ed invio di una notifica "aggregata" invece che singole comunicazioni;

- scoperta di più violazioni che coinvolgono le stesse tipologie di dati avvenute a breve distanza l'una dall'altra.

L'esigenza dell'aggregazione di più notifiche non comporta necessariamente un ritardo nella notifica all'Autorità.

Processo di comunicazione agli interessati

Sulla base della valutazione precedentemente descritta al paragrafo precedente, quando la Violazione dei Dati Personali possa comportare un rischio elevato per i diritti e le libertà degli Interessati o su richiesta dell'Autorità, Digital Bros S.p.A., dopo aver prontamente notificato l'evento al Garante, comunica la Violazione dei Dati Personali agli stessi Interessati senza indebito ritardo.

Il **Comitato per la gestione dei Data Breach** stabilisce il canale più appropriato per inviare questa comunicazione (es. e-mail, SMS, telefono, ecc.).

Nei casi in cui sia coinvolto un numero molto elevato di contraenti Digital Bros S.p.A. informerà, non appena ragionevolmente possibile e in stretta collaborazione con l'Autorità di controllo (Considerando 86 del GDPR), i soggetti i cui dati sono coinvolti dalla violazione tramite forme di comunicazione di carattere pubblico, quali la diffusione di avvisi su quotidiani, anche online, oppure mediante altri strumenti disponibili.

La comunicazione all'interessato deve almeno:

- descrivere, con un linguaggio semplice e chiaro, la natura della violazione dei dati personali includendo, ove possibile, le categorie e il numero approssimativo di soggetti interessati, nonché le categorie e il numero approssimativo di record di dati personali interessati;
- comunicare il nome e i dettagli di contatto del DPO o altro punto di contatto presso cui è possibile ottenere ulteriori informazioni;
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o di cui si propone l'adozione per fronteggiare la violazione dei dati personali, comprese, se del caso, suggerire agli stessi le misure per mitigarne i possibili effetti negativi.

MONITORAGGIO DELLE VIOLAZIONI

La fase di monitoraggio delle violazioni prevede le seguenti attività:

- Il Responsabile Sistemi Informatici o il Responsabile SISTEMI Fisici che ha segnalato l'incidente inerente alla gestione dei propri archivi / sicurezza fisica e/o logica al Responsabile Privacy (con il supporto di eventuali funzioni preposte) analizza costantemente quanto accaduto e fornisce informazioni aggiuntive ed aggiornate,

attivandosi per risolvere quanto accaduto e aggiornando il Comitato sull'andamento della gestione e della risoluzione del Data Breach;

- Il Comitato per la gestione dei Data Breach monitora l'andamento e l'evoluzione della violazione chiedendo e ricevendo di volta in volta informazioni aggiuntive e necessarie; inoltre, il Comitato valuta le misure di mitigazione necessarie per la protezione dei dati personali degli Interessati;
- Il Responsabile Sistemi Informatici o il Responsabile SISTEMI Fisici a cui si riferisce l'incidente inerente alla gestione degli archivi fisici/sicurezza fisica, dopo aver identificato e posto rimedio alla o alle vulnerabilità evolute in Data Breach, supporta il DPO nella compilazione e nell'aggiornamento costante del Registro dei Data Breach , per quanto riguarda:
    - descrizione del Data Breach;
    - natura della violazione;
    - analisi delle cause principali;
    - piano di azione mirato alla messa in sicurezza dei dati personali;
    - azioni correttive implementate o in fase di implementazione.
- Il Comitato per la gestione dei Data Breach informa il Titolare della chiusura e della risoluzione della Violazione;
- Il DPO una volta che il processo di valutazione è concluso e tutte le informazioni sono state raccolte, predispone un report di chiusura del Data Breach; tale report deve contenere almeno:
    - Descrizione della natura del Data Breach;
    - Data e ora in cui è stato rilevato il Data Breach;
    - Chi / cosa ha segnalato il Data Breach;
    - Numero approssimativo e categoria di Interessati coinvolti;
    - Numero approssimativo e categoria dei Dati Personali violati;
    - Dettagli di qualsiasi sistema IT coinvolto;
    - Archivi fisici o dispositivi rimovibili coinvolti;
    - Meccanismi di sicurezza in atto al momento del Data Breach;
    - Possibili conseguenze del Data Breach;
    - Misure adottate o adottabili.
- Il Responsabile Sistemi Informatici o il Responsabile Sistemi Fisici implementa altresì le misure di sicurezza individuate.
- Il DPO assieme ai membri del Comitato per la gestione dei Data Breach valuta le necessità formative dei dipendenti, in particolare con riferimento a quanto emerso dall'analisi dall'avvenuta violazione.

- Il DPO gestisce la corrispondenza ed i riscontri ricevuti dall'Autorità come, ad esempio, modalità e tempi per la comunicazione agli interessati, misure di sicurezza da mettere in atto, ecc.

Nell'ambito delle attività di monitoraggio dei Data Breach è prevista la gestione di un registro (registro dei Data Breach) contenente tutte le informazioni relative alle Violazioni che, come minimo, contiene:

- la documentazione relativa ai Data Breach (informazioni raccolte, valutazioni effettuate e ogni altro materiale a supporto della valutazione, come ad esempio messaggi di errore, LOG, ecc.);
- la notifica delle Violazioni all'Autorità;
- la comunicazione delle Violazioni agli Interessati, ove applicabile;
- feedback ricevuti dall'Autorità.

GESTIONE DEL REGISTRO DEI DATA BREACH

Al fine di consentire all'Autorità di verificare il rispetto della normativa, il DPO registra e archivia qualsiasi violazione dei dati personali all'intero del Registro dei Data Breach, inserendo anche gli eventi per i quali si è deciso di non procedere alla notificazione e delle ragioni di questa scelta.

Il Registro dei Data Breach dovrà essere continuamente aggiornato e messo a disposizione dell'Autorità, qualora questa chieda di consultarlo.

Dovranno, inoltre, essere adottate idonee misure atte a garantire l'integrità e la non modificabilità delle registrazioni in esso contenute.

DATA RETENTION

PRINCIPI GENERALI

Il presente paragrafo ha lo scopo di descrivere i tempi di conservazione delle diverse tipologie dei dati personali di cui Digital Bros S.p.A. è Titolare, e che sono trattati dalle diverse figure aziendali nominate incaricati della gestione dei dati personali, conformemente a quanto previsto dalla normativa vigente in tema di protezione dei dati personali (Regolamento UE 2016/679).

Il documento si applica ai dati di:

- Candidati;
- Dipendenti;
- Clienti B2C & B2B;
- Fornitori;
- Visitatori.

Il documento fornisce le indicazioni necessarie alla cancellazione dei dati, a seconda del periodo di conservazione indicato. Le prescrizioni valgono inoltre per tutte le terze parti (clienti, fornitori, consulenti, agenti, ecc.) che partecipano alle attività di conservazione e cancellazione dei dati personali di titolarità di Digital Bros S.p.A..

CONSERVAZIONE DEI DATI PERSONALI

Digital Bros S.p.A. deve definire il periodo di conservazione dei dati personali, al termine del quale la cancellazione o l'anonimizzazione devono essere effettuate secondo le disposizioni legislative e regolamentari applicabili. Tali disposizioni legislative e regolamentari potrebbero avere requisiti specifici relativi ai trattamenti effettuati sui dati personali (e.g. attività di marketing o profilazione).

Digital Bros S.p.A. deve almeno:

- conservare i dati personali solo per il tempo necessario al completamento delle attività per le quali i dati sono stati raccolti e che sono state dichiarate all'interno dell'informativa privacy consegnata agli interessati;
- conservare i dati personali assicurando la compliance rispetto al consenso ottenuto dall'individuo e ai requisiti contrattuali e legislativi;
- cancellare i dati personali qualora richiesto da requisiti normativi locali;
- cancellare i dati personali qualora l'interessato voglia esercitare il diritto di cancellazione di tutti i dati personali che lo riguardano senza ingiustificato ritardo ("diritto alla cancellazione") e comunicare la richiesta dell'interessato e a qualsiasi terza parte alla quale i dati personali sono stati comunicati, se applicabile.

Inoltre, a seguito di una richiesta di cancellazione da parte dell'interessato, Digital Bros S.p.A. deve garantire tale diritto quando vale almeno uno dei seguenti punti:

- i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
- l'interessato revoca il consenso su cui si basa il trattamento e se non sussiste altro fondamento giuridico per il trattamento;
- l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento;
- i dati personali sono stati trattati illecitamente;
- i dati personali devono essere cancellati per adempiere un obbligo legale previsto dalle disposizioni legislative e regolamentari nazionali cui Digital Bros S.p.A. è soggetta;

- la conservazione dei dati personali viola le disposizioni legislative e regolamentari nazionali cui Digital Bros S.p.A. è soggetta.

L'interessato potrebbe inoltre esercitare il proprio diritto alla portabilità. In tal caso, esso non modifica automaticamente il periodo di conservazione definito e non causa automaticamente la cancellazione dei dati personali dai sistemi Digital Bros S.p.A., sino a quando una richiesta specifica non è presentata dall'interessato. Nel caso in cui l'Interessato esercitasse, invece, il diritto alla limitazione, l'eventuale decorrenza del termine o altre condizioni che potrebbero richiedere la cancellazione dei dati resterebbero sospese sino alla cessazione del vincolo stesso.

CANCELLAZIONE DEI DATI PERSONALI

Al termine del periodo di conservazione, Digital Bros S.p.A. deve cancellare i dati personali raccolti secondo le disposizioni legislative e regolamentari applicabili.

Digital Bros S.p.A. deve inoltre comunicare, senza ingiustificato ritardo, a qualsiasi terza parte coinvolta nelle attività di trattamento dei dati personali di procedere con la cancellazione degli stessi.

Qualora la cancellazione dei dati venga effettuata, Digital Bros S.p.A. non deve ulteriormente trattare tali dati personali. Per questo motivo, Digital Bros S.p.A. deve implementare processi e meccanismi per garantire una revisione periodica dei periodi di cancellazione e i limiti di tempo definitivi per la cancellazione dei dati personali vengano rispettati, internamente ed esternamente (e.g. dalle terze parti che trattano dati personali), includendo specifiche clausole contrattuali che permettano a Digital Bros S.p.A. di condurre attività di audit.

Digital Bros S.p.A. deve inoltre assicurarsi che tutti i dispositivi elettronici dove i dati personali sono stati conservati vengano, al termine del loro ciclo di vita, accuratamente dismessi, al fine di prevenire qualsiasi accesso non autorizzato alle informazioni conservate al loro interno.

DATA RETENTION

Le tabelle riportate nel prosieguo del documento contengono l'indicazione del periodo di conservazione dei dati trattati con riferimento alle diverse categorie di interessati:

- Candidati
- Dipendenti
- Clienti B2C & B2B
- Fornitori
- Visitatori
- Altro

Il periodo di conservazione ivi indicato tiene conto di eventuali disposizioni normative previste al riguardo o di indicazioni specifiche fornite dall'Autorità nei provvedimenti dallo stesso emanati nel corso degli anni.

In assenza di indicazioni fornite dalla normativa applicabile o dal Garante Privacy in ordine al periodo di conservazione dei dati personali trattati, lo stesso è stato individuato valutando quale potesse essere un periodo congruo, nel rispetto del principio secondo cui i dati personali dovrebbero essere conservati per il periodo di tempo strettamente necessario al completamento delle attività per le quali essi sono stati raccolti.

Infine, si fa presente che tutti i dati che non rientrano nelle categorie sottoelencate dovranno essere oggetto di valutazione da parte del DPO e del Responsabile Privacy, al fine di individuarne il corretto periodo di conservazione.

A. DATI DEI CANDIDATI

CANDIDATI			
Descrizione e finalità	**Tipologia dei dati**	**Periodo di conservazione**	**Riferimenti normativi**
Dati personali ordinari e/o "particolari" contenuti nei curricula, trattati a fini di selezione del personale	Anagrafica, dati di contatto, eventuale appartenenza a categorie protette, esperienze professionali, istruzione	6 mesi dall'ultimo caricamento del CV	-
Dati personali ordinari trattati per la gestione e l'accoglienza dei soggetti che accedono alla sede aziendale	Anagrafica	3 mesi	-

B. DATI DEI DIPENDENTI

DIPENDENTI			
Descrizione e finalità	**Tipologia dei dati**	**Periodo di conservazione**	**Riferimenti normativi**
Dati personali ordinari e/o "particolari" inerenti alla gestione dei dipendenti trattati ai fini di gestione del rapporto contrattuale (ad esempio la gestione delle buste paga trattati ai fini di gestione del rapporto contrattuale, ecc.)	Anagrafica, dati di contatto, contratto di lavoro, cartella personale del dipendente, documentazione disciplinare, copia del documento d'identità e del titolo di studio, adesione a sindacati, attestati di partecipazione a corsi di formazione, buste paga, compensi, benefits, regime pensionistico, dati di retribuzione	Almeno 10 anni dopo la fine del rapporto contrattuale, salva la conservazione a fini fiscali	*Tale periodo è determinato in base all'art. 43 del Dpr 600/73 e all'art. 2946 codice civile sulla prescrizione ordinaria**
Dati personali ordinari trattati per la gestione di reclami e contenziosi	Anagrafica, dati di contatto, contratto di lavoro, cartella personale del dipendente, documentazione disciplinare, copia del documento d'identità e del titolo di studio, adesione a sindacati, attestati di partecipazione a corsi di formazione, buste paga, compensi, benefits, regime pensionistico, dati di retribuzione	Almeno 10 anni dopo la fine del rapporto contrattuale (per conservare i dati necessari per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria)	*Tale periodo è determinato in base all'art. 2946 codice civile sulla prescrizione ordinaria. **

DIPENDENTI			
Descrizione e finalità	**Tipologia dei dati**	**Periodo di conservazione**	**Riferimenti normativi**
Dati personali ordinari e/o "particolari" relativi agli aspetti di salute/sanitari trattati ai fini di gestione del rapporto contrattuale	Anagrafica, dati di contatto, dati di presenza/assenza, certificati di malattia, idoneità, inabilità, congedo di paternità/maternità, dichiarazioni di infortunio sul lavoro	Almeno 10 anni dopo la fine del rapporto contrattuale	*Tale periodo è determinato in base all'art. 2946 codice civile sulla prescrizione ordinaria e agli artt. 25 "Medico competente", 41 "Sorveglianza sanitaria" e 53 "Tenuta della documentazione" del D.lgs.81/08 e s.m.i.**
Dati personali ordinari, per la gestione del tracciamento delle attività degli AdS, trattati ai fini di gestione del rapporto contrattuale	Log di accesso a livello sistemistico e applicativo per il monitoraggio delle attività degli AdS	Minimo 6 mesi fino a un massimo di 24 mesi dalla generazione del log stesso	*Provv.to Garante "amministratori di sistema" del 28/11/08 e s.m.i.**
Dati personali ordinari trattati per la gestione dell'account di posta elettronica del dipendente	Nome, cognome, dati di contatto, *job title*, indirizzo e - mail	Per tutta la durata del rapporto di lavoro e disattivazione dell'account di posta elettronica alla cessazione del rapporto di lavoro entro 30 giorni, secondo modalità tali da inibire in via definitiva la ricezione in entrata di messaggi diretti all'account dell'ex dipendente, nonché la conservazione degli stessi su server aziendali	-

DIPENDENTI			
Descrizione e finalità	**Tipologia dei dati**	**Periodo di conservazione**	**Riferimenti normativi**
Dati personali trattati tramite sistemi di videosorveglianza a fini di sicurezza e tutela del patrimonio aziendale	Immagini	Massimo 48 ore	*Provv.to generale del Garante privacy del 08/4/2010*
Dati personali degli amministratori di Digital Bros S.p.A. e del nucleo familiare (eccetto i figli minorenni) ai fini del rilascio delle dichiarazioni necessarie alla partecipazione ai bandi di gara pubblici (es. dichiarazione antimafia).	Anagrafica, dati di contatto, dati giudiziari, dati fiscali	Almeno 10 anni dopo la fine del rapporto contrattuale	-

C. DATI DEI CLIENTI B2C

CLIENTI B2C			
Descrizione e finalità	**Tipologia dei dati**	**Periodo di conservazione**	**Riferimenti normativi**
Dati personali ordinari trattati per finalità di marketing diretto dei clienti	Anagrafica, dati di contatto	2 anni dalla revoca del consenso	-
Dati personali ordinari e particolari trattati per finalità di *customer caring* (Facebook,)	Anagrafica, dati di contatto,	2 anni dall'evasione della richiesta del cliente.	-

CLIENTI B2C			
Descrizione e finalità	**Tipologia dei dati**	**Periodo di conservazione**	**Riferimenti normativi**
Dati personali ordinari trattati per la gestione di reclami e contenziosi	Anagrafica, dati di contatto, dati di fatturazione	Almeno 10 anni dopo la fine del rapporto contrattuale (per conservare i dati necessari per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria)	*Tale periodo è determinato in base all'art. 2946 codice civile sulla prescrizione ordinaria. **

D. DATI DEI CLIENTI B2B

CLIENTI B2B			
Descrizione e finalità	**Tipologia dei dati**	**Periodo di conservazione**	**Riferimenti normativi**
Dati personali ordinari di Clienti B2B	Anagrafica, dati di contatto, dati di fatturazione	3 anni dalla fine del rapporto commerciale	-
Dati personali ordinari trattati per finalità di gestione contabile del canale di vendita e per il contrasto alle frodi	Anagrafica, dati di contatto, dati di fatturazione	Almeno 5 anni dopo la fine del rapporto contrattuale	*Tale periodo è determinato in base all'art. 2948 codice civile che prevede la prescrizione di 5 anni per i pagamenti periodici. **
Dati personali ordinari trattati per finalità di gestione amministrativa e fiscale e per la gestione di reclami e contenziosi	Anagrafica, dati di contatto, dati di fatturazione, contratti di beni e servizi, fatture di beni e servizi, polizze assicurative/fideiussorie, elenco Clienti, permessi, licenze, certificazioni,	Almeno 10 anni dopo la fine del rapporto contrattuale	*Tale periodo è determinato in base all'art. 2946, 2220 codice civile e all'art. 22 del D.P.R. 29 Settembre 1973, n.600 (obblighi civilistici dell'imprenditore di*

CLIENTI B2B			
Descrizione e finalità	**Tipologia dei dati**	**Periodo di conservazione**	**Riferimenti normativi**
	accordi di confidenzialità/MOU.		*conservazione delle scritture contabili e della corrispondenza commerciale; obblighi di conservazione a fini fiscali). **
Dati personali ordinari trattati per la gestione e l'accoglienza dei soggetti che accedono alla sede aziendale	Anagrafica	3 mesi	-

E. DATI DEI FORNITORI / CONSULENTI ESTERNI

FORNITORI / CONSULENTI ESTERNI			
Descrizione e finalità	**Tipologia dei dati**	**Periodo di conservazione**	**Riferimenti normativi**
Dati personali ordinari trattati per la gestione di reclami e contenziosi	Anagrafica, dati di contatto, dati di fatturazione	Almeno 10 anni dopo la fine del rapporto contrattuale	*Tale periodo è determinato in base all'art. 2946 codice civile sulla prescrizione ordinaria. **
Dati personali ordinari trattati per la gestione amministrativa e fiscale	Anagrafica, dati di contatto, contratti di beni e servizi, fatture di beni e servizi, polizze assicurative e fideiussorie, elenco Clienti e Fornitori, permessi, licenze, certificazioni, accordi di confidenzialità/MOU.	Almeno 10 anni dopo la fine del rapporto contrattuale	*Tale periodo è determinato in base all'art. 2220 codice civile e all'art. 22 del D.P.R. 29 Settembre 1973, n.600 (obblighi civilistici dell'imprenditore di conservazione delle scritture contabili e della*

FORNITORI / CONSULENTI ESTERNI			
Descrizione e finalità	**Tipologia dei dati**	**Periodo di conservazione**	**Riferimenti normativi**
			*corrispondenza commerciale; obblighi di conservazione a fini fiscali). **
Dati personali ordinari, per la gestione del tracciamento delle attività degli AdS, trattati ai fini di gestione del rapporto contrattuale	Log di accesso a livello sistemistico e applicativo per il monitoraggio delle attività degli AdS	Minimo 6 mesi fino a un massimo di 24 mesi dalla generazione del log stesso	*Provv.to Garante "amministratori di sistema" del 28/11/08 e s.m.i.**
Dati personali ordinari trattati per la gestione e l'accoglienza dei soggetti che accedono alla sede aziendale	Anagrafica	3 mesi	-
Dati personali ordinari inerenti alla gestione dei consulenti esterni trattati ai fini di gestione del rapporto contrattuale, dei reclami e contenziosi e ai fini amministrativi/fiscali	Anagrafica, dati di contatto, dati di fatturazione, contratti di beni e servizi, fatture di beni e servizi, polizze assicurative e fideiussorie, elenco Clienti e Fornitori, permessi, licenze, certificazioni	Almeno 10 anni dopo la fine del rapporto contrattuale	*Tale periodo è determinato in base all'art. 2946 codice civile sulla prescrizione ordinaria e all'art. 2220 codice civile e all'art. 22 del D.P.R. 29 Settembre 1973, n.600 (obblighi civilistici dell'imprenditore di conservazione delle scritture contabili e della corrispondenza commerciale; obblighi di conservazione a fini fiscali). **

F. DATI DEI VISITATORI

VISITATORI			
Descrizione e finalità	**Tipologia dei dati**	**Periodo di conservazione**	**Riferimenti normativi**
Dati personali ordinari trattati per la gestione e l'accoglienza dei soggetti che accedono alla sede aziendale	Anagrafica, eventuale società di appartenenza	3 mesi	-
Dati personali trattati tramite sistemi di videosorveglianza a fini di sicurezza e tutela del patrimonio aziendale	Immagini	48 ore	*Provv.to generale del Garante privacy del 08/4/2010*

ESEMPI DI TECNICHE DI CANCELLAZIONE DEI DATI E DISMISSIONE DEI DISPOSITIVI

Le specifiche attività di cancellazione dei dati e di dismissione dei dispositivi devono essere condotte al fine di garantire che i dati personali non siano più accessibili al termine del loro ciclo di vita.

Le tecniche di cancellazione sicura dei dati possono includere, tra le altre:

- Cancellazione sicura delle informazioni, ottenibile con programmi informatici (quali *wiping program* o *file shredder*) che provvedono, una volta che l'utente abbia eliminato dei file da un'unità disco o da analoghi supporti di memorizzazione con i normali strumenti previsti dai diversi sistemi operativi, a scrivere ripetutamente nelle aree vuote del disco (precedentemente occupate dalle informazioni eliminate) sequenze casuali di cifre "binarie" (zero e uno) in modo da ridurre al minimo le probabilità di recupero di informazioni anche tramite strumenti elettronici di analisi e recupero di dati;
- Formattazione "a basso livello" dei dispositivi di tipo hard disk (*low-level formatting–LLF*), laddove effettuabile, attenendosi alle istruzioni fornite dal produttore del dispositivo e tenendo conto delle possibili conseguenze tecniche su di esso, fino alla possibile sua successiva inutilizzabilità;
- Demagnetizzazione (*degaussing*) dei dispositivi di memoria basati su supporti magnetici o magneto-ottici (dischi rigidi, floppy-disk, nastri magnetici su bobine aperte o in cassette), in grado di garantire la cancellazione rapida delle informazioni anche su dispositivi non più

funzionanti ai quali potrebbero non essere applicabili le procedure di cancellazione software (che richiedono l'accessibilità del dispositivo da parte del sistema a cui è interconnesso).

Tecniche di dismissione sicura dei dispositivi possono includere, tra le altre:

- sistemi di punzonatura o deformazione meccanica;
- distruzione fisica o di disintegrazione (usata per i supporti ottici come CD-ROM e DVD);
- demagnetizzazione ad alta intensità.

Si richiede ai fornitori di consegnare un certificato relativo all'effettiva esecuzione dell'attività di cancellazione secondo procedure standard quali ISO 27001 e ISO 27040.

GESTIONE DELLE RICHIESTE DI ESERCIZIO DEI DIRITTI DA PARTE DELL'INTERESSATO

PRINCIPI GENERALI

Per l'esercizio delle richieste avanzate dagli interessati, Digital Bros S.p.A. prevede l'utilizzo di indirizzi mail dedicati dpo@digitalbros.com - privacy@digitalbros.com con cui saranno evase le risposte, nel rispetto dei processi di gestione della privacy.

Gli interessati, tuttavia, potrebbero avanzare le loro richieste anche attraverso altri canali, ed esattamente:

- casella postale (posta raccomandata);
- form di contatto disponibile sui siti web del gruppo Digital Bros.

In questi casi, la funzione aziendale / terza parte incaricata alla gestione del canale utilizzato dall'interessato ha il compito di inoltrare la richiesta all'indirizzo mail dedicato non appena ricevuta la richiesta.

IDENTIFICAZIONE DEL RICHIEDENTE

La prima fase del processo prevede l'identificazione del richiedente; a tal fine, infatti, è necessario che l'interessato abbia indicato i propri dati anagrafici e i propri recapiti, nonché ogni informazione utile per il suo riconoscimento.

Una volta ricevuta la richiesta, con il supporto delle relative funzioni alle quali si associa la gestione della richiesta da parte dell'interessato, il Responsabile Privacy coadiuvato dal DPO verifica (entro 10 giorni solari) la consistenza e la tipologia delle informazioni possedute. Qualora l'interessato non sia identificabile in maniera univoca, si richiederà allo stesso di completare la richiesta con le informazioni utili alla sua identificazione.

Naturalmente l'esigenza di "identificare l'Interessato" va vista anche in funzione della tipologia di diritto esercitata e, conseguentemente, degli eventuali dati personali che potrebbero essere resi disponibili.

Al termine delle operazioni di identificazione, il DPO, non appena verrà formulata una risposta a riguardo, avrà cura di comunicare all'interessato il relativo riscontro rispetto alla richiesta in questione.

RACCOLTA E VERIFICA DEI DATI

Terminata la fase di identificazione dell'Interessato, il DPO avvierà le attività di raccolta delle informazioni riguardanti l'interessato, che dovranno concludersi entro 20 giorni solari dalla ricezione della richiesta. A tal fine saranno coinvolte le funzioni di competenza per la raccolta/estrazione dei dati necessari.

In particolare, le richieste possono arrivare con riferimento ai seguenti ambiti:

- dati dei Clienti, sulla base della specifica richiesta potrà essere coinvolta la funzione **Marketing;**
- dati dei Dipendenti e del personale autonomo, anche al termine del rapporto di lavoro, in questo caso potrà essere coinvolta la funzione **Amministrazione** o **HR**.

Inoltre, le specifiche Funzioni di competenza, nella persona del rispettivo Privacy Owner, dovranno essere coinvolte per la raccolta di eventuali informazioni possedute da Terze Parti che trattano dati per conto di Digital Bros S.p.A. e per la raccolta di eventuali informazioni contenute nei propri archivi.

Le funzioni di competenza si rivolgono al Responsabile Sistemi Informatici per l'estrazione dei dati.

Una volta raccolti ed organizzati i dati, il DPO, con il supporto dei Privacy Owner e del Responsabile Privacy, provvederà a verificarne la congruenza dei dati, le tipologie e le modalità di trattamento svolte, nonché la presenza dei relativi consensi.

PREDISPOSIZIONE DEL RISCONTRO

Raccolti e verificati i dati in possesso del Titolare (e di eventuali terze parti Responsabili del trattamento) il DPO e le funzioni preposte (nella persona del rispettivo Privacy Owner) gestiscono la richiesta e redigono la risposta relativa al diritto esercitato secondo le modalità in seguito descritte, entro 30 giorni (solari) dalla ricezione della richiesta. Tale termine può essere prorogato fino a 60 giorni (solari), tenuto conto della complessità e del numero delle richieste, fermo restando l'obbligo di informare l'Interessato di tale proroga e dei motivi del ritardo entro 30 giorni (solari) dalla ricezione della richiesta. L'approvazione dell'applicazione della proroga dev'essere fornita dal DPO.

Se la richiesta inviata dall'Interessato ha in copia il Garante, le comunicazioni necessarie saranno inviate con in copia il Garante. Qualora, invece, fosse il Garante a richiedere informazioni, le comunicazioni necessarie, a valle delle attività di analisi effettuate, saranno inviate direttamente al Garante.

In base alla specifica richiesta ricevuta potrà essere eventualmente coinvolto il Responsabile Sistemi Informatici per la gestione delle richieste degli interessati (es. cancellazione dei dati dai sistemi, limitazione del trattamento, portabilità).

A. DIRITTO DI ACCESSO

Esercitando il diritto di accesso, l'interessato può ottenere la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano. In tal caso può accedere a tali dati e ottenere, se richieste, informazioni relative alle finalità del trattamento, al periodo di conservazione dei dati personali (o, se non è possibile, i criteri utilizzati per definire tale periodo) o anche all'esistenza di un processo decisionale automatizzato, compresa la profilazione. L'interessato, inoltre, può richiedere la copia dei dati personali oggetto di trattamento.

Sulla base dei dati raccolti il DPO identifica, in collaborazione con le funzioni preposte le informazioni da fornire all'Interessato e predispone la risposta.

La risposta deve essere inviata all'Interessato anche nel caso in cui la richiesta di esercizio del diritto di accesso non possa essere accolta. In tal caso, la risposta deve contenere le specifiche motivazioni e deve essere condivisa anche con il Resp. Privacy.

B. DIRITTO DI RETTIFICA

Con l'esercizio di questo diritto, l'interessato può ottenere (anche in seguito ad una richiesta di esercizio del diritto di accesso) la rettifica delle informazioni inesatte che lo riguardano. L'interessato ha, inoltre, la facoltà di integrare eventuali dati personali incompleti, tenuto conto delle finalità del trattamento.

Nel caso in cui un Interessato richieda la rettifica e/o l'integrazione dei propri Dati Personali sono previste le seguenti modalità (a titolo esemplificativo e non esaustivo):

- dati dei clienti: la valutazione sulla possibilità di eseguire la rettifica, la gestione operativa della richiesta e la predisposizione della risposta è eseguita direttamente dalla funzione preposta con il supporto del DPO e del Responsabile Sistemi Informativi;
- dati dei dipendenti e del personale autonomo: la valutazione sulla possibilità di eseguire la rettifica, la gestione operativa della richiesta e la predisposizione della risposta è eseguita direttamente dalla funzione Amministrazione HR, con il supporto del DPO e del Responsabile Sistemi Informativi.

In tale contesto potrebbe essere necessario coinvolgere altre funzioni aziendali o Terze Parti che gestiscono ulteriori archivi fisici o sistemi riguardanti l'Interessato di riferimento.

Nel caso di coinvolgimento di terze parti si deve richiedere un riscontro formale sull'avvenuta esecuzione della richiesta.

La risposta deve essere inviata all'Interessato anche nel caso in cui la richiesta di esercizio del diritto di rettifica non possa essere accolta. In tal caso la risposta deve contenere le specifiche motivazioni e deve essere condivisa anche con il Responsabile Privacy.

C. DIRITTO ALLA CANCELLAZIONE

L'esercizio di questo diritto prevede la cancellazione di tutti i dati personali relativi all'interessato. In seguito alla raccolta e verifica dei dati in possesso del Titolare (o di eventuali Responsabili Esterni), la richiesta sarà processata se:

- I dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti;
- L'interessato revoca il consenso su cui si basa il trattamento e non sussiste altro fondamento giuridico per il trattamento;
- L'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per proseguire nel trattamento,
- L'interessato si oppone al trattamento per finalità di marketing (ai sensi dell'articolo 21, paragrafo 2);
- I dati personali sono stati trattati illecitamente;
- I dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del trattamento.

Nel caso in cui un Interessato richieda la cancellazione dei propri Dati Personali sono previste le seguenti modalità:

- Dati dei clienti: la valutazione sulla possibilità di eseguire la cancellazione, la gestione operativa della richiesta e la predisposizione della risposta viene eseguita direttamente dalla funzione interessata con il supporto del DPO e del Responsabile Sistemi Informativi;
- Dati dei dipendenti e del personale autonomo: la valutazione sulla possibilità di eseguire la cancellazione, la gestione operativa della richiesta e la predisposizione della risposta viene eseguita direttamente dalla funzione Amministrazione HR, con il supporto del DPO e del Responsabile Sistemi Informativi.

In tale contesto potrebbe essere necessario coinvolgere altre funzioni aziendali o Terze Parti che gestiscono ulteriori archivi fisici o sistemi riguardanti l'Interessato di riferimento. Nel caso di coinvolgimento di terze parti si deve richiedere un riscontro formale sull'avvenuta cancellazione.

La risposta deve essere inviata all'Interessato anche nel caso in cui la richiesta di esercizio del diritto alla cancellazione non possa essere accolta. In tal caso la risposta deve contenere le specifiche motivazioni e deve essere condivisa anche con il Responsabile Privacy.

D. DIRITTO DI LIMITAZIONE AL TRATTAMENTO

Il diritto di limitazione del trattamento prevede che l'utilizzo dei dati e, quindi, il trattamento, sia limitato a quanto necessario ai fini della conservazione; questo diritto è esercitabile in alcuni casi particolari:

- nel caso in cui l'interessato contesti l'esattezza dei dati personali, per il periodo necessario al Titolare del trattamento per verificarne l'esattezza;
- se, in presenza di un trattamento illecito, l'interessato si opponga alla cancellazione dei dati personali, chiedendo che al posto della cancellazione sia disposta la limitazione del loro utilizzo;
- laddove il titolare del trattamento non abbia più bisogno o intenzione di conservare i dati, ma sussista la necessità di mantenerli in quanto necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
- in caso di opposizione al trattamento, nell'attesa delle verifiche necessarie alla determinazione della prevalenza dei motivi legittimi del Titolare del trattamento o dei diritti dell'interessato.

In questi casi, quindi, i dati devono essere trattati solo ai fini della loro conservazione, salvo che vi sia il consenso dell'interessato al trattamento per fini diversi, o il trattamento sia necessario per l'esercizio o la difesa di un diritto in sede giudiziaria, per la tutela dei diritti di un'altra persona fisica o giuridica o per motivi di interesse.

Qualora la richiesta dell'interessato non possa essere processata (ai sensi di quanto previsto dal GDPR), il DPO provvede a comunicare all'interessato l'impossibilità di dare seguito alla sua richiesta: in tal caso, la risposta deve contenere le specifiche motivazioni e deve essere condivisa anche con il Responsabile Privacy.

Se, invece, dovesse essere necessario dare seguito alla richiesta, il DPO coinvolgerà le funzioni competenti, tramite i relativi Privacy Owner, al fine di:

- Contrassegnare e rendere inaccessibili i dati da tutti i sistemi aziendali e non permettere ulteriori operazioni di trattamento;
- Raccogliere tutti i dati in formato cartaceo ed organizzarli in una sezione dedicata;
- Comunicare ai Responsabili esterni i dati personali oggetto del diritto e ricevere da questi un riscontro sull'avvenuta limitazione.

I dati limitati potranno essere poi sbloccati (quindi si potrà proseguire con il trattamento) solo con il consenso espresso dell'interessato, oppure potranno essere trattati – senza consenso – solo ed esclusivamente per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica.

Al termine delle attività, il DPO provvede a comunicare al richiedente l'esito della richiesta. L'interessato che ha ottenuto la limitazione del trattamento, inoltre, è informato prima che detta limitazione sia revocata.

E. DIRITTO ALLA PORTABILITÀ DI DATI

L'interessato, con l'esercizio di tale diritto, potrà richiedere in un formato strutturato i dati che lo riguardano se:

- il trattamento si basi sul consenso o su un contratto;
- il trattamento sia effettuato con mezzi automatizzati.

Tutte le richieste ricevute devono essere gestite dal DPO. A seguito della richiesta e della verifica dei dati posseduti, il DPO, con il supporto delle funzioni preposte, individua tra le informazioni raccolte quali sono i Dati Personali per i quali può avvenire la portabilità.

La funzione preposta, con l'eventuale supporto del Responsabile Sistemi Informativi, provvede a fornire al DPO l'estrazione dei dati in formato strutturato (con particolare riferimento ai dati forniti dallo stesso Interessato), esclusivamente nel caso in cui siano stati identificati dei Dati Personali per cui è applicabile tale diritto.

Qualora l'Interessato richieda espressamente che tali informazioni siano trasferite presso un altro Titolare del trattamento, il DPO con il supporto delle funzioni competenti provvederà a contattare quest'ultimo al fine di definire le modalità della trasmissione. In questo caso la richiesta potrà essere evasa solo se tecnicamente possibile.

Al termine delle attività, il DPO provvede a comunicare l'esito della richiesta all'Interessato, trasmettendo all'Interessato o presso un altro Titolare del trattamento la documentazione prodotta secondo quanto concordato.

La risposta deve essere inviata all'Interessato anche nel caso in cui la richiesta di esercizio del diritto alla portabilità di dati non possa essere accolta. In tal caso la risposta deve contenere le specifiche motivazioni e deve essere condivisa anche con il Coordinatore Privacy.

F. DIRITTO DI OPPOSIZIONE

Con l'esercizio di questo diritto l'interessato può opporsi in qualsiasi momento al trattamento dei dati che lo riguardano, compresi i trattamenti connessi a ragioni di interesse pubblico o posti in essere per il

perseguimento di interessi legittimi del Titolare. Tutte le richieste ricevute devono essere gestite dal DPO. Una volta ricevuta la richiesta, raccolti e verificati i dati posseduti, il DPO procederà a verificare l'esistenza di motivazioni legittime per continuare a procedere con il trattamento ai sensi di quanto previsto dal GDPR. In caso affermativo, il DPO comunica all'interessato l'impossibilità di dare seguito alla sua richiesta, specificando nel dettaglio le motivazioni.

In caso contrario, invece, il DPO con il supporto delle funzioni competenti e del Responsabile Sistemi Informativi, individua tra le informazioni raccolte quali sono i dati personali per i quali può essere esercitato il diritto di opposizione e, procedere secondo quanto richiesto dall'interessato.

Inoltre, i Privacy Owner delle specifiche funzioni di competenza dovranno essere coinvolti per la raccolta di eventuali informazioni possedute da Terze Parti che trattano dati per conto di Digital Bros S.p.A. e per la raccolta di eventuali informazioni contenute negli archivi gestiti da quest'ultima.

L'interessato, inoltre, può opporsi anche al trattamento dei dati per finalità commerciali (come marketing diretto e profilazione); in questi casi i dati personali non saranno più oggetto di trattamento per tali finalità. A tal fine, per determinate tipologie di attività e trattamenti (ad esempio newsletter e simili) Digital Bros S.p.A. predispone appositi sistemi automatizzati per la revoca del consenso (es. pulsante ***unsubscribe*** nelle newsletter).

Al termine delle suddette attività, il DPO provvederà a comunicare al richiedente l'esito della propria richiesta.

ARCHIVIAZIONE DELLE RICHIESTE

Le richieste di esercizio di diritti da parte degli Interessati vengono mappate su un documento sulla base del Modello– Gestione richieste Interessati.