Titolare del Trattamento: Servizi polifunzionali ecosostenibili Gioia s.p.a.

Sede legale: Via Gabriele D'Annunzio n. 76/78 - 70023 Gioia Del Colle (BA)

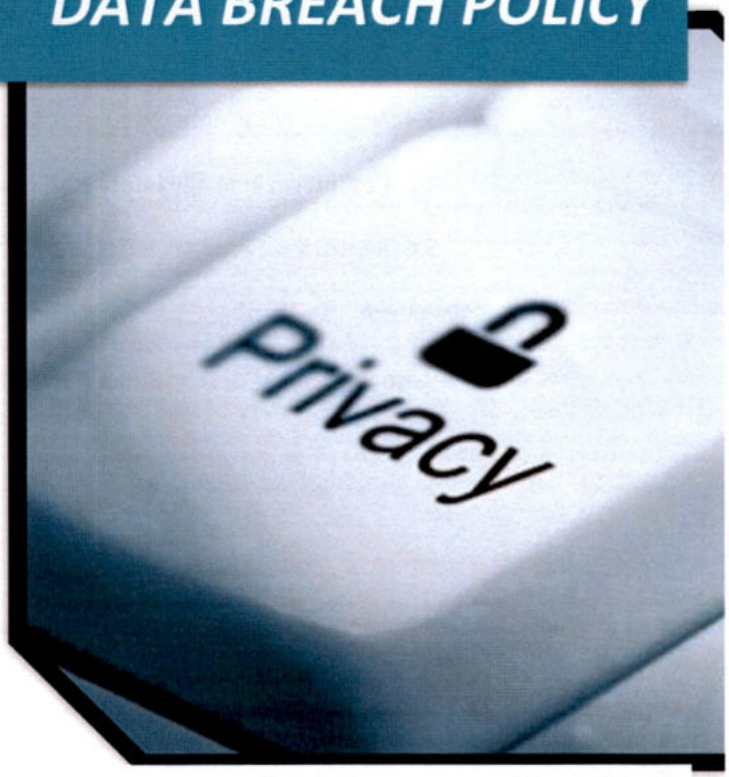
P.IVA: 06245760720

N. telefono: 0803481667

Email: info@spesspa.com

PEC: spesspa@pec.it

DATA BREACH POLICY



Responsabile della Protezione dei Dati (DPO)

Opera Professioni srl

rpd@spesspa.com

Via Gabriele D'Annunzio n. 76/78 - 70023 Gioia Del Colle (BA)

Data emissione: 20/05/2019

Sommario

1. Premessa

Con i termini *"DATA BREACH"* si intende una breccia nella sicurezza che ha come conseguenza la distruzione, la perdita, la modifica, la divulgazione senza autorizzazione o l'accesso ai dati personali (conservati, trasmessi o trattati con qualunque modalità) avvenuta in seguito a un evento accidentale, oppure in seguito a un atto illecito.

Il Gruppo di lavoro ex art. 29 ha individuato tre differenti tipi di violazione dei dati personali, confermandoli nelle linee guida adottate dapprima nell'ottobre 2017 e successivamente revisionate nel febbraio 2018:

- "**Violazione della riservatezza**": che si verifica in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali;
- "**Violazione dell'integrità**": ravvisabile qualora vi sia un'alterazione non autorizzata o accidentale dei dati personali;
- "**Violazione della disponibilità**": eventualità riguardante la perdita accidentale o non preventivata, l'accesso o distruzione nei confronti dei dati personali.

Talvolta una singola violazione ben può integrare tutte e tre le eventualità sopra definite. Inoltre, un incidente di sicurezza che porti a rendere indisponibili i dati personali per un limitato periodo di tempo potrebbe costituire anch'esso un tipo di violazione, visto il significativo impatto che potrebbe avere sui diritti e le libertà fondamentali delle persone fisiche. È sempre necessario valutare il caso specifico (ad esempio, un intervento di manutenzione programmata dei sistemi che renda inaccessibili i dati per il tempo necessario non è identificabile come una violazione).

Le violazioni di dati personali possono accadere per un ampio numero di ragioni che possono includere:

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

Le conseguenze di un *Data breach*, lungi dall'essere circoscrivibili ad un solo danno relativo alla sicurezza, possono ben sfociare in lesioni particolarmente rilevanti nei confronti degli interessati i cui dati risultano violati. Il *Data breach*, richiede quindi un intervento tempestivo volto alla limitazione di conseguenze quali danni fisici, materiali o immateriali

alle persone fisiche. Nello specifico potrebbe verificarsi una costrizione dei diritti degli interessati, una loro discriminazione (si pensi alla sottrazione di particolari categorie di dati, ad esempio afferenti alla vita sessuale, alle convinzioni politiche o religiose, all'origine etnica etc.), furto o usurpazione di identità, un danno economico, una lesione della reputazione, una lesione del segreto professionale ovvero qualsiasi tipo di ulteriore danno di tipo economico o sociale di rilievo ai danni della persona fisica interessata.

2. Scopo e ambito di applicazione

Lo scopo del presente documento è disciplinare la corretta gestione delle eventuali violazioni dei dati personali trattati (*data breach*) nel rispetto della normativa in materia di trattamento dei dati personali, garantendo in particolare l'aderenza ai principi e alle disposizioni contenute nel Regolamento (UE) 2016/679.

Il presente documento è rivolto a tutti i soggetti che, a qualsiasi titolo, trattano dati personali di competenza del Titolare del trattamento. A titolo esemplificativo:

- i lavoratori dipendenti, nonché coloro che, indipendentemente dal tipo di rapporto lavorativo intercorrente, abbiano accesso ai dati personali trattati nel corso del proprio impiego per conto del Titolare del trattamento (genericamente denominati autorizzati);
- i soggetti (persone fisiche o giuridiche) che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento, abbiano accesso ai suddetti dati e agiscano in qualità di Responsabile del trattamento ex art. 28 GDPR.

I destinatari devono obbligatoriamente attenersi al contenuto del presente documento. Il mancato rispetto e la mancata conformità alle regole previste potrà comportare provvedimenti disciplinari a carico dei dipendenti inadempienti ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia, fermo restando il risarcimento di eventuali danni causati.

A tal proposito, tutti i destinatari sono debitamente informati delle regole contenute nel presente documento mediante metodi e mezzi che ne assicurino la comprensione.

3. Definizioni

Ai fini della corretta comprensione dei paragrafi successivi, si riportano le seguenti definizioni:

Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia digitalizzato o meno, centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

Autorità di controllo: autorità pubblica e indipendente insignita di tale ruolo da uno stato membro. In Italia è il Garante per la protezione dei dati personali;

Autorizzato al trattamento: la persona fisica, espressamente designata, che opera sotto l'autorità del titolare del trattamento, con specifici compiti e funzioni connessi al trattamento dei dati personali;

Dato personale: qualsiasi tipo di informazione inerente a una persona fisica, sia essa identificata o identificabile (interessato). È definibile come identificabile, la persona fisica che sia possibile identificare direttamente o indirettamente, ad esempio tramite il nome oppure un numero identificativo;

Destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo a cui vengono inviati dati personali, di terzi o meno. Non sono da considerarsi destinatari le autorità pubbliche a cui possono essere inviate comunicazioni di dati personali nell'ambito di una specifica indagine in accordo con l'assetto normativo dell'Unione e degli Stati membri;

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

GDPR: *General Data Protection Regulation*, noto anche come Regolamento Generale sulla Protezione dei Dati (RGPD), ovvero Regolamento UE 679/2016 (di seguito anche solo "Regolamento");

Pseudonimizzazione: trattamento dei dati personali posto in essere in maniera tale che gli stessi non siano riferibili a un interessato specifico senza l'ausilio di informazioni supplementari. Tali informazioni, al fine di garantire la tutela che ci si propone, devono essere conservate separatamente e soggette a misure tecniche e organizzative volte a garantire che i dati non siano riferibili a una persona fisica identificata, o identificabile;

Responsabile del trattamento: colui (persona fisica o giuridica, autorità pubblica, il servizio o altro organismo) che tratta i dati personali per conto del titolare;

Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo al di fuori dell'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate a trattare i dati sotto l'autorità del titolare o del responsabile;

Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo, che in autonomia o con altri soggetti determina le finalità e le modalità del trattamento dei dati personali; In questo contesto, è Titolare del trattamento Servizi polifunzionali ecosostenibili Gioia s.p.a.

Trattamento: qualsiasi operazione o insieme di operazioni, poste in essere con o senza l'ausilio di processi automatizzati e utilizzate su dati personali o insiemi di dati personali.

Rientrano nei trattamenti, la raccolta, la registrazione, la conservazione, la cancellazione, la consultazione, l'invio, la comunicazione, l'uso, la distruzione, la limitazione etc..

4. Ambito normativo

Il presente documento è redatto in conformità alle disposizioni di legge e alla normativa vigente. In particolare:

- Regolamento (UE) n. 2016/679;
- *Guidelines on Personal data breach notification under Regulation 2016/679 – article 29 data protection working party (Adopted on 3 October 2017 – as last Revised and Adopted on 6 February 2018).*

L'art. 32 del GDPR prevede che, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, il titolare e il responsabile del trattamento mettano in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

Nella valutazione del livello di sicurezza bisognerà tener conto in special modo dei rischi presentati dal trattamento che potrebbero derivare dalla distruzione, dalla perdita, dalla modifica o dalla divulgazione non autorizzata o dall'accesso in modo accidentale o illegale ai dati personali trasmessi, conservati o comunque trattati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale agli Interessati.

L'art. 33 e 34 del GDPR disciplinano gli obblighi del Titolare in caso di violazione dei dati personali.

Le linee guida del WP29 forniscono importanti indicazioni sul comportamento da adottare in caso di violazione dei dati e sulla valutazione da effettuare anche ai fini della eventuale notificazione al Garante e comunicazione agli interessati.

5. Procedura per la gestione e segnalazione della violazione

Le violazioni di dati personali sono gestite dal Titolare del trattamento o da un suo delegato, sotto la supervisione del DPO.

5.1. Rilevazione e segnalazione delle violazioni

In caso di concreta, sospetta e/o avvenuta violazione dei dati personali, è necessario assicurare che essa sia affrontata immediatamente e correttamente al fine di minimizzare l'impatto della violazione e prevenire un'eventuale ripetizione della stessa.

A tale scopo, è stato predisposto un modulo che i destinatari dovranno utilizzare per la comunicazione delle eventuali violazioni (Allegato A – Modulo *Data Breach*), secondo le seguenti modalità.

Segnalazione interna

Qualora uno degli autorizzati - lavoratori dipendenti o, indipendentemente dalla tipologia contrattuale, un soggetto interno che presta attività secondo le direttive del Titolare (tirocinante, studente, etc.) - si accorga di una concreta, potenziale o sospetta violazione dei dati personali, dovrà immediatamente informare dell'incidente il superiore gerarchico (ove presente).

Il superiore gerarchico si occuperà, con il supporto dei segnalanti stessi, di raccogliere tutte le informazioni necessarie per la compilazione del modulo (Allegato A – Modulo *Data Breach*) e procederà ad informare il Titolare del trattamento o un suo delegato trasmettendo, a mezzo e-mail all'indirizzo *info@spesspa.com*, il modulo stesso debitamente compilato secondo le istruzioni presenti.

In mancanza del superiore gerarchico, gli autorizzati provvederanno direttamente alla compilazione trasmissione del succitato modulo all'indirizzo suindicato.

Segnalazione esterna

Ogni Responsabile esterno è obbligato da contratto ad informare il titolare del trattamento senza ingiustificato ritardo, di ogni potenziale evento di *data breach*. A tal proposito, nell'atto volto a disciplinare il rapporto ai sensi dell'art. 28 del Regolamento (UE) n. 2016/679, sono inserite apposite istruzioni da seguire in caso di violazione dei dati, compreso il modulo da compilare e trasmettere al Titolare.

Pertanto, ogni responsabile del trattamento, qualora venga a conoscenza di una concreta, potenziale o sospetta violazione dei dati che riguardi dati che egli tratta per conto del Titolare, procederà a informare il Titolare mediante l'invio del modulo nei tempi indicati nell'atto succitato (entro 24 ore dalla conoscenza dell'eventuale violazione da parte del responsabile).

5.2. Valutazione e classificazione della violazione

Una volta ricevuti i moduli debitamente compilati, il Titolare del trattamento (o il suo delegato), con il coinvolgimento del DPO, effettuerà una valutazione iniziale riguardante la notizia dell'incidente occorso, al fine di stabilire se si sia effettivamente verificata un'ipotesi di *Data Breach* (violazione) e se sia necessaria un'indagine più approfondita dell'accaduto.

Qualora la violazione riguardi dati contenuti in un sistema informatico, il Titolare del trattamento (o il suo delegato) dovrà necessariamente coinvolgere nella valutazione e nella fasi successive documento anche il Responsabile IT, o un suo delegato in caso di assenza.

Ai fini di una corretta valutazione e classificazione dell'episodio, il Titolare (o il suo delegato) utilizzerà le indicazioni contenute nell'Allegato B (Linee guida in caso di violazione dei dati).

5.3. Azioni correttive

Sulla scorta delle determinazioni raggiunte in sede di valutazione e classificazione, il Titolare del trattamento (o il suo delegato), di concerto con il DPO, dovranno stabilire:

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

5.4. Notifica al Garante (ove necessaria)

Qualora dalla valutazione effettuata dovesse emergere la necessità di effettuare la notificazione all'Autorità, il Titolare del trattamento e il DPO procederanno a trasmettere, ai sensi dell'art. 33 del Regolamento (UE) n. 2016/679, le relative informazioni all'Autorità di Controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore, da determinarsi dal momento in cui il Titolare ne è venuto a conoscenza, cioè quando abbia un ragionevole grado di certezza della verificazione di un incidente di sicurezza che riguardi dati personali. Oltre il termine delle 72 ore, la notifica deve essere corredata delle ragioni del ritardo.

In ogni caso, è fatta salva la possibilità di fornire successivamente all'Autorità informazioni aggiuntive o dettagli rilevanti sulla violazione di cui il Titolare venga a conoscenza, a seguito della effettuazione di ulteriori indagini e attività successive.

La scelta e le motivazioni sulla base delle quali il Titolare stabilisce di non notificare l'evento deve essere documentata nell'apposito registro indicato nel presente documento.

5.5. Comunicazione agli interessati (ove necessaria)

Nel caso in cui dal la violazione possa derivare un rischio elevato per i diritti e le libertà delle persone (interessati), il Titolare dovrà informare le stesse senza ingiustificato ritardo, al fine di consentire loro di prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione.

L'eventuale comunicazione all'interessato/agli interessati dovrà contenere:

- il nome e i dati di contatto del Responsabile della protezione dei dati (DPO);
- la descrizione delle probabili conseguenze della violazione dei dati personali;
- la descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e, se del caso, per attenuarne i possibili effetti negativi.

Il Titolare, anche attraverso il supporto del DPO, individuerà i tempi e le modalità di comunicazione più opportune ai sensi dell'art. 34 del Regolamento (UE) n. 2016/679, tenendo conto di eventuali indicazioni fornite dall'Autorità Garante. In ogni caso, dovranno essere privilegiate forme di comunicazione diretta con i soggetti interessati (quali email, SMS o messaggi diretti). Il messaggio dovrà essere comunicato in maniera evidente e trasparente, evitando inserire le informazioni nel contesto di informazioni generali o newsletter, che potrebbero essere facilmente fraintesi dai lettori. Nel caso in cui la segnalazione diretta richieda uno sforzo ritenuto sproporzionato, allora si potrà utilizzare una comunicazione pubblica, che dovrà essere ugualmente efficace nel contatto diretto con l'interessato.

5.6. Registrazione della violazione

Qualsiasi violazione verificatasi, indipendentemente dalla necessità di procedere alla notificazione al Garante e/o comunicazione agli interessati, dovrà essere annotata nell'apposito registro istituito, gestito e conservato dal Titolare ai sensi dell'art. 33, comma 5 del GDPR.

Tale registro, costituito da un file excel, dovrà essere compilato in tutti i suoi campi, secondo le istruzioni *quivi* contenute, costantemente aggiornato e messo a disposizione dell'Autorità Garante su richiesta della stessa.

Allegato A – Modulo Data Breach

Allegato A – Modulo Data Breach	
Soggetto compilatore	
Data e ora della violazione	
Data e orario in cui si è venuti a conoscenza della violazione dei dati	
Circostanze in cui è avvenuta la violazione	
Tipologia di dati violati	
Categorie di interessati colpiti dalla violazione	
Conseguenze della violazione	
Numero(anche approssimativo) dei dati violati	
Numero(anche approssimativo) degli interessati colpiti	
Provvedimenti adottati per porvi rimedio	
Note	

Istruzioni per la compilazione del modulo

Allegato A – Modulo Data Breach (esempio)	
Soggetto compilatore	*Inserire il nome e cognome del soggetto che compila il modulo al fine di effettuare la segnalazione*
Data e ora della violazione	*Indicare la data e l'ora in cui (anche presumibilmente) è avvenuta la violazione, specificando se si sia prolungata e per quanto*
Data e orario in cui si è venuti a conoscenza della violazione dei dati	*Indicare la data e l'ora in cui il soggetto segnalatore è venuto a conoscenza della violazione*
Circostanze in cui è avvenuta la violazione	*Indicare le modalità ed eventuali altre informazioni inerenti alla violazione (es. violazione avvenuta in seguito ad attacco informatico ad opera di un haker; furto all'interno dell'edificio ad opera di soggetti non identificati; Invio errato di dati a mezzo Email da parte di Tizio, autorizzato al trattamento; oppure, incendio con relativa distruzione di archivi cartacei; oppure smarrimento di chiavetta usb)*
Tipologia di dati violati	*Indicare se i dati violati sono: comuni, particolari, giudiziari ovvero appartenenti a minori; specificare se possono rientrare in più di una delle categorie elencate; specificare, se possibile, il tipo di dato nello specifico (es. cartella clinica, esami medici, documentazione contenente informazioni inerenti alle credenze religiose, appartenenze politiche, appartenenze sindacali, origine etnica, ecc.; dati comuni: nome, cognome, indirizzo ecc.; dati giudiziari: documentazione relativa a procedimenti giudiziari, condanne penali etc.)*
Categorie di interessati colpiti dalla violazione	*Indicare le categorie di interessati colpiti dalla violazione: clienti, fornitori, lavoratori, etc.*
Conseguenze della violazione	*Indicare le conseguenze derivanti dalla violazione(es. divulgazione di dati personali degli interessati; danni alla struttura; danni ai device aziendali; perdita di accesso al database; impossibilità di accedere ai dati a causa di una crittografia generata da soggetti esterni; impossibilità temporanea di porre in essere gli adempimenti aziendali etc.)*
Numero(anche approssimativo) dei dati violati	*Indicare il numero dei dati violati, anche in maniera approssimativa grazie a una stima sommaria)*
Numero(anche approssimativo) degli interessati colpiti	*Indicare il numero dei soggetti che hanno visto i propri dati violati, anche in maniera approssimativa grazie a una stima sommaria)*
Provvedimenti adottati per porvi rimedio	*Indicare eventuali provvedimenti successivi alla violazione volti ad arginare i danni o ad eliminarne le conseguenze negative e la data di adozione degli stessi (es. ripristino del database grazie a copie di backup; avvio delle indagini per verificare le dinamiche dell'accaduto ed eventuali profili di responsabilità; pulizia del sistema dai malware; aggiornamento della politica aziendale riguardo la protezione dei dati personali; predisposizione di misure cautelative per evitare il ripetersi dell'evento; etc.)*
Note	*Indicare eventuali aggiornamenti: (es. confronto successivo con il DPO, con l'Autorità di controllo etc.)*

Allegato B - Linee guida in caso di violazione dei dati

In caso di avvenuta violazione, ai fini di una corretta valutazione, il Titolare procederà come segue.

Articolo 33 – Notifica di una violazione dei dati personali all'autorità di controllo

L'art. 33 del GDPR stabilisce che in caso di violazione dei dati personali, il titolare del trattamento debba notificare la violazione all'autorità di controllo (il Garante per la protezione dei dati personali) senza ingiustificato ritardo, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Si ritiene che il titolare del trattamento debba considerarsi "a conoscenza" nel momento in cui è ragionevolmente certo che si è verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali. Il titolare del trattamento è quindi tenuto a prendere le misure necessarie per assicurarsi di venire "a conoscenza" di eventuali violazioni in maniera tempestiva in modo da poter adottare le misure appropriate.

Esempi

1. In caso di perdita di una chiave USB contenente dati personali non crittografati spesso non è possibile accertare se persone non autorizzate abbiano avuto accesso ai dati. Tuttavia, anche se il titolare del trattamento non è in grado di stabilire se si è verificata una violazione della riservatezza, tale caso deve essere notificato, in quanto sussiste una ragionevole certezza del fatto che si è verificata una violazione della disponibilità; il titolare del trattamento si considera venuto "a conoscenza" della violazione nel momento in cui si è accorto di aver perso la chiave USB.

2. Un terzo informa il titolare del trattamento di aver ricevuto accidentalmente i dati personali di uno dei suoi clienti e fornisce la prova della divulgazione non autorizzata. Dato che al titolare del trattamento è stata presentata una prova evidente di una violazione della riservatezza, non vi è dubbio che ne sia venuto "a conoscenza".

3. Un titolare del trattamento rileva che c'è stata una possibile intrusione nella sua rete. Controlla quindi i propri sistemi per stabilire se i dati personali ivi presenti sono stati compromessi e ne ottiene conferma. Ancora una volta, dato che il titolare del trattamento ha una chiara prova di una violazione non può esserci dubbio che sia venuto "a conoscenza" della stessa.

4. Un criminale informatico viola il sistema del titolare del trattamento e lo contatta per chiedere un riscatto. In tal caso, dopo aver verificato il suo sistema per accertarsi dell'attacco, il titolare del trattamento dispone di prove evidenti che si è verificata una violazione e non vi è dubbio che ne sia venuto a conoscenza.

Dopo che il titolare del trattamento è venuto a conoscenza di una violazione soggetta a notifica, la stessa deve essere notificata senza ingiustificato ritardo e, ove possibile, entro 72 ore. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, la stessa deve essere corredata dei motivi del ritardo.

Nel notificare una violazione all'autorità di controllo, l'articolo 33, paragrafo 3 stabilisce che la notifica deve almeno:

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

Articolo 34 – Comunicazione di una violazione dei dati personali all'interessato

L'articolo 34, paragrafo 1, afferma che quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento debba comunicare la violazione all'interessato senza ingiustificato ritardo, il che significa il prima possibile.
L'obiettivo principale della comunicazione agli interessati consiste nel fornire loro informazioni specifiche sulle misure che questi possono prendere per proteggersi.
Ai fini della comunicazione alle persone fisiche, l'articolo 34, paragrafo 2, specifica che:
"La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d)".
Secondo tale disposizione, il titolare del trattamento deve fornire almeno le seguenti informazioni:

1. una descrizione della natura della violazione;
2. il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto;
3. una descrizione delle probabili conseguenze della violazione;
4. una descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

I Contitolari ed i Responsabili del trattamento
L'articolo 26 riguarda i contitolari del trattamento e specifica che essi devono determinare le rispettive responsabilità in merito all'osservanza del regolamento. Ciò includerà la determinazione di chi sarà responsabile di adempiere agli obblighi di cui agli articoli 33 e 34.
Il Gruppo di lavoro raccomanda che gli accordi contrattuali tra i contitolari del trattamento includano disposizioni che stabiliscano quale titolare del trattamento assumerà il comando o sarà responsabile del rispetto degli obblighi di notifica delle violazioni previsti dal regolamento.

Sebbene il titolare del trattamento conservi la responsabilità generale per la protezione dei dati personali, il responsabile del trattamento svolge un ruolo importante nel consentire al titolare del trattamento di adempiere ai propri obblighi, segnatamente in materia di notifica delle violazioni. L'articolo 28, paragrafo 3, dispone che il trattamento da parte di un responsabile del trattamento è disciplinato da un contratto o da un altro atto giuridico, e precisa, alla lettera f), che il contratto o altro atto giuridico deve prevedere che il responsabile del trattamento "assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento".

La valutazione dell'esistenza di un rischio o di un rischio elevato

È doveroso specificare come non sia obbligatorio notificare una violazione in tutte le circostanze, nello specifico:

- la notifica all'autorità di controllo competente (art. 33 GDPR) è obbligatoria a meno che sia improbabile che la violazione possa presentare un rischio per i diritti e le libertà delle persone fisiche;
- la comunicazione di una violazione alle persone fisiche (art. 34 GDPR) diventa necessaria soltanto laddove la violazione possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

La notifica di una violazione è obbligatoria a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche, mentre la comunicazione di una violazione agli interessati deve essere effettuata se è probabile che la violazione presenti un rischio *elevato* per i diritti e le libertà delle persone fisiche. Tale rischio sussiste quando la violazione può comportare un danno fisico, materiale o immateriale per le persone fisiche i cui dati sono stati violati.
Esempi di tali danni sono la discriminazione, il furto o l'usurpazione d'identità, perdite finanziarie e il pregiudizio alla reputazione. Il verificarsi di tale danno dovrebbe essere considerato probabile quando la violazione riguarda dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, oppure che includono dati genetici, dati relativi alla salute o dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza.
I considerando 75 e 76 del regolamento suggeriscono che, di norma, nella valutazione del rischio si dovrebbero prendere in considerazione tanto la probabilità quanto la gravità del rischio per i diritti e le libertà degli interessati. Inoltre il regolamento afferma che il rischio dovrebbe essere valutato in base a una valutazione oggettiva.

Fattori da considerare nella valutazione del rischio.

1) Tipo di violazione

- Una violazione della riservatezza che ha portato alla divulgazione di informazioni mediche a soggetti non autorizzati può avere conseguenze diverse per una persona fisica rispetto a una violazione in cui i dettagli medici di una persona fisica sono stati persi e non sono più disponibili

2) Natura, carattere sensibile e volume dei dati personali

- Un elemento fondamentale della valutazione del rischio sono il tipo e il carattere sensibile dei dati personali che sono stati compromessi dalla violazione. Solitamente più i dati sono sensibili, maggiore è il rischio di danni per le persone interessate; tuttavia si dovrebbero prendere in considerazione anche altri dati personali che potrebbero già essere disponibili sull'interessato Violazioni relative a dati sulla salute, documenti di identità o dati finanziari come i dettagli di carte di credito, possono tutte causare danni di per sé, ma se tali dati fossero usati congiuntamente si potrebbe avere un'usurpazione d'identità. Di norma una combinazione di dati personali ha un carattere più sensibile rispetto a un singolo dato personale.

3) Facilità di identificazione delle persone fisiche

- Un fattore importante da considerare è la facilità con cui un soggetto che può accedere a dati personali compromessi riesce a identificare persone specifiche o ad abbinare i dati con altre informazioni per identificare persone fisiche. A seconda delle circostanze, l'identificazione potrebbe essere possibile direttamente dai dati personali oggetto di violazione senza che sia necessaria alcuna ricerca speciale per scoprire l'identità dell'interessato, oppure potrebbe essere estremamente difficile abbinare i dati personali a una particolare persona fisica, ma sarebbe comunque possibile a determinate condizioni.

4) Gravità delle conseguenze per le persone fisiche

- A seconda della natura dei dati personali coinvolti in una violazione, ad esempio categorie particolari di dati, il danno potenziale alle persone che potrebbe derivarne può essere particolarmente grave soprattutto se la violazione può comportare furto o usurpazione di identità, danni fisici, disagio psicologico, umiliazione o danni alla reputazione. Se la violazione riguarda dati personali relativi a persone fisiche vulnerabili, queste ultime potrebbero essere esposte a un rischio maggiore di danni.
  Il fatto che il titolare del trattamento sappia o meno che i dati personali sono nelle mani di persone le cui intenzioni sono sconosciute o potenzialmente dannose può incidere sul livello di rischio potenziale.

5) Caratteristiche particolari dell'interessato

- Una violazione può riguardare dati personali relativi a minori o ad altre persone fisiche vulnerabili, che possono di conseguenza essere soggette a un rischio più elevato di danno. Altri fattori concernenti la persona fisica potrebbero influire sul livello di impatto della violazione sulla stessa.

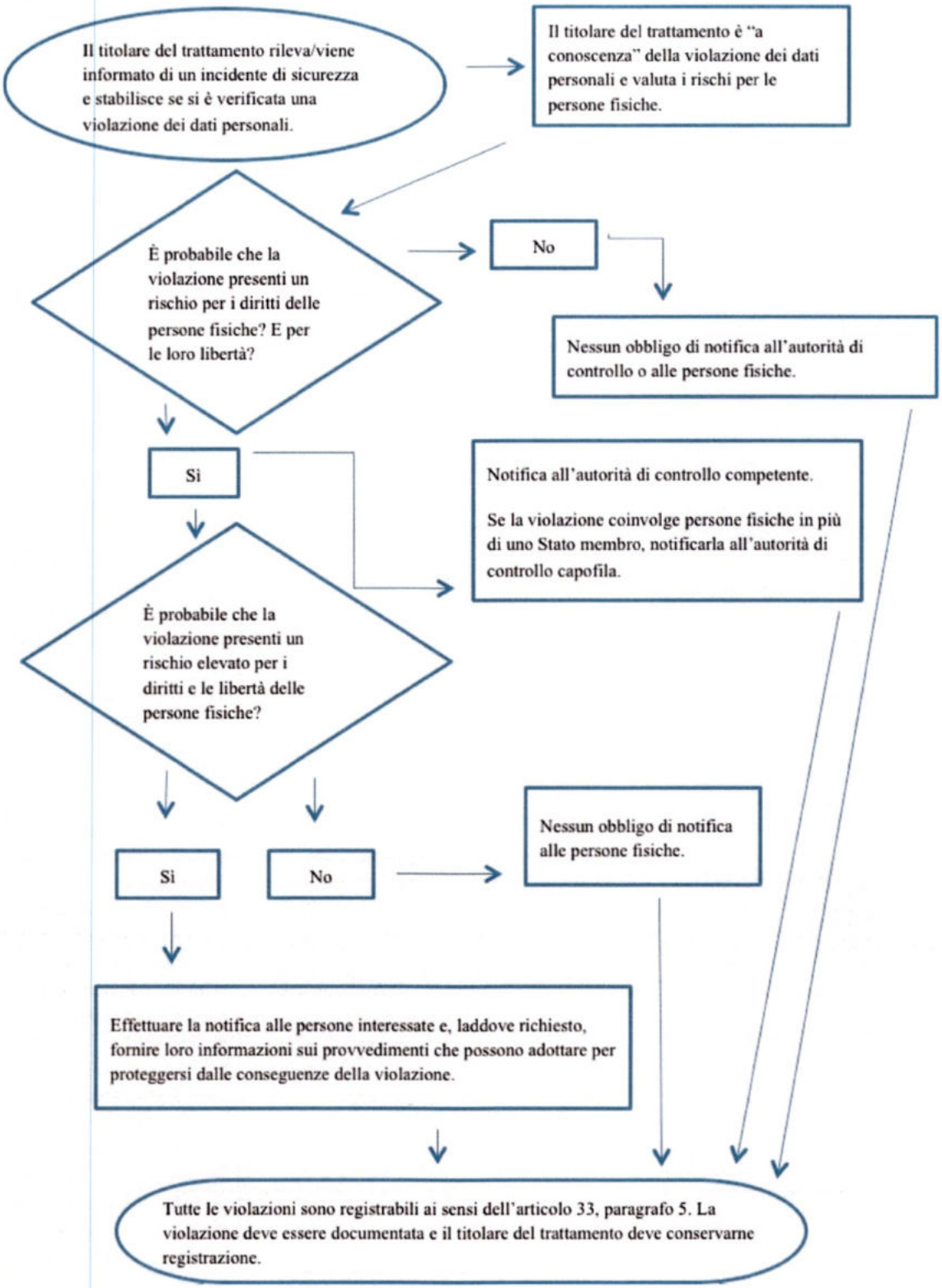
6) Caratteristiche particolari del titolare del trattamento di dati

- La natura e il ruolo del titolare del trattamento e delle sue attività possono influire sul livello di rischio per le persone fisiche in seguito a una violazione. Ad esempio, un'organizzazione medica tratterà categorie particolari di dati personali, il che significa che vi è una minaccia maggiore per le persone fisiche nel caso in cui i loro dati personali vengano violati, rispetto a una mailing list di un quotidiano.

7) Numero di persone fisiche interessate

- Una violazione può riguardare solo una o poche persone fisiche oppure diverse migliaia di persone fisiche, se non molte di più. Di norma, maggiore è il numero di persone fisiche interessate, maggiore è l'impatto che una violazione può avere. Tuttavia, una violazione può avere ripercussioni gravi anche su una sola persona fisica, a seconda della natura dei dati personali e del contesto nel quale i dati sono stati compromessi. Ancora una volta, l'aspetto fondamentale consiste nel considerare la probabilità e la gravità dell'impatto sulle persone interessate.

Diagramma relativo all'obbligo di notifica:



Esempi di violazioni dei dati personali e relative conseguenze:

Esempio	Notifica all'autorità di controllo?	Comunicazione all'interessato?	Note/raccomandazioni
Un titolare del trattamento ha effettuato un backup di un archivio di dati personali crittografati su una chiave USB. La chiave viene rubata durante un'effrazione.	No.	No.	Fintantoché i dati sono crittografati con un algoritmo all'avanguardia, esistono backup dei dati, la chiave univoca non viene compromessa e i dati possono essere ripristinati in tempo utile, potrebbe non trattarsi di una violazione da segnalare. Tuttavia, se la chiave viene successivamente compromessa, è necessaria la notifica.
ii. Un titolare del trattamento gestisce un servizio online. A seguito di un attacco informatico ai danni di tale servizio, i dati personali di persone fisiche vengono prelevati. Il titolare del trattamento ha clienti in un solo Stato membro.	Sì, segnalare l'evento all'autorità di controllo se vi sono probabili conseguenze per le persone fisiche.	Sì, segnalare l'evento alle persone fisiche a seconda della natura dei dati personali interessati e se la gravità delle probabili conseguenze per tali persone è elevata.	
iii. Una breve interruzione di corrente di alcuni minuti presso il call center di un titolare del trattamento impedisce ai clienti di chiamare il titolare del trattamento e accedere alle proprie registrazioni.	No.	No.	Questa non è una violazione soggetta a notifica, ma costituisce comunque un incidente registrabile ai sensi dell'articolo 33, paragrafo 5. Il titolare del trattamento deve conservare adeguate registrazioni in merito.
iv. Un titolare del trattamento subisce un attacco tramite *ransomware* che provoca la cifratura di tutti i dati. Non sono disponibili backup e i dati non possono essere ripristinati. Durante le indagini, diventa evidente che l'unica funzionalità dal *ransomware* era la cifratura dei dati e che non vi erano altri *malware* presenti nel sistema.	Sì, effettuare la segnalazione all'autorità di controllo, se vi sono probabili conseguenze per le persone fisiche in quanto si tratta di una perdita di disponibilità.	Sì, effettuare la segnalazione alle persone fisiche, a seconda della natura dei dati personali interessati e del possibile effetto della mancanza di disponibilità dei dati, nonché di altre possibili conseguenze.	Se fosse stato disponibile un backup e i dati avessero potuto essere ripristinati in tempo utile non sarebbe stato necessario segnalare la violazione all'autorità di controllo o alle persone fisiche, in quanto non si sarebbe verificata nessuna perdita permanente di disponibilità o di riservatezza. Tuttavia, qualora l'autorità di controllo fosse venuta a conoscenza dell'incidente con altri mezzi, avrebbe potuto prendere in considerazione lo svolgimento di un'indagine al fine di valutare il rispetto dei requisiti di sicurezza più ampi di cui all'articolo 32.
v. Una persona telefona al call center di una banca per segnalare una violazione dei dati. La persona ha ricevuto	Sì.	La comunicazione va effettuata soltanto alle persone fisiche coinvolte in caso di rischio elevato e se è	Se dopo ulteriori indagini si stabilisce che l'evento ha interessato un numero maggiore di persone fisiche è necessario comunicare questo sviluppo

l'estratto conto mensile da un soggetto diverso. Il titolare del trattamento intraprende una breve indagine (ossia la conclude entro 24 ore) e stabilisce con ragionevole certezza che si è verificata una violazione dei dati personali e che vi è una potenziale carenza sistemica che potrebbe comportare il coinvolgimento già occorso o potenziale di altre persone fisiche.		evidente che altre persone fisiche non sono state interessate dall'evento.	all'autorità di controllo, e il titolare del trattamento deve informarne le altre persone fisiche interessate se sussiste un rischio elevato per loro.
vi. Un titolare del trattamento gestisce un mercato online e ha clienti in più Stati membri. Tale mercato subisce un attacco informatico a seguito del quale i nomi utente, le password e la cronologia degli acquisti vengono pubblicati online dall'autore dell'attacco.	Sì, segnalare l'evento all'autorità di controllo capofila se la violazione riguarda un trattamento transfrontaliero.	Sì, dato che la violazione potrebbe comportare un rischio elevato.	Il titolare del trattamento dovrebbe prendere delle misure, ad esempio forzare il ripristino delle password degli account interessati, e altri provvedimenti per attenuare il rischio. Il titolare del trattamento dovrebbe altresì considerare qualsiasi altro obbligo di notifica, ad esempio ai sensi della direttiva NIS, trattandosi di un fornitore di servizi digitali.
vii. Una società di *hosting* di siti web che funge da responsabile del trattamento individua un errore nel codice che controlla l'autorizzazione dell'utente. A causa di tale vizio, qualsiasi utente può accedere ai dettagli dell'account di qualsiasi altro utente.	In veste di responsabile del trattamento, la società di *hosting* di siti web deve effettuare la notifica ai clienti interessati (i titolari del trattamento) senza ingiustificato ritardo. Supponendo che la società di *hosting* di siti web abbia condotto le proprie indagini, i titolari del trattamento interessati dovrebbero essere ragionevolmente certi di aver subito una violazione e pertanto è probabile che vengano considerati "a conoscenza" della violazione nel momento in cui hanno ricevuto la notifica da parte della società di *hosting* (il	Qualora non vi siano probabili rischi elevati per le persone fisiche non è necessario effettuare una comunicazione a tali persone.	La società di *hosting* di siti web (responsabile del trattamento) deve prendere in considerazione qualsiasi altro obbligo di notifica (ad esempio ai sensi della direttiva NIS, trattandosi di un fornitore di servizi digitali). Qualora non vi sia alcuna prova che tale vulnerabilità sia sfruttata presso uno dei suoi titolari del trattamento, la violazione potrebbe non essere soggetta all'obbligo di notifica, tuttavia potrebbe essere una violazione da registrare o essere il segno di un mancato rispetto dell'articolo 32.

	responsabile del trattamento). Il titolare del trattamento deve quindi effettuare la notifica all'autorità di controllo.		
viii. Le cartelle cliniche di un ospedale sono indisponibili per un periodo di 30 ore a causa di un attacco informatico.	Sì, l'ospedale è tenuto a effettuare la notifica in quanto può verificarsi un rischio elevato per la salute e la tutela della vita privata dei pazienti.	Sì, informare le persone fisiche coinvolte.	
ix. I dati personali di un gran numero di studenti vengono inviati per errore a una mailing list sbagliata con più di 1 000 destinatari.	Sì, segnalare l'evento all'autorità di controllo.	Sì, segnalare l'evento alle persone fisiche coinvolte in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze.	
x. Una e-mail di marketing diretto viene inviata ai destinatari nei campi "a:" o "cc:", consentendo così a ciascun destinatario di vedere l'indirizzo e-mail di altri destinatari.	Sì, la notifica all'autorità di controllo può essere obbligatoria se è interessato un numero elevato di persone, se vengono rivelati dati sensibili (ad esempio una mailing list di uno psicoterapeuta) o se altri fattori presentano rischi elevati (ad esempio, il messaggio di posta elettronica contiene le password iniziali).	Sì, segnalare l'evento alle persone fisiche coinvolte in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze.	La notifica potrebbe non essere necessaria se non vengono rivelati dati sensibili e se viene rivelato soltanto un numero limitato di indirizzi di posta elettronica.

Cookie Policy – Informazioni

Le presenti informazioni, rese ai sensi dell'art. 13 del Regolamento Europeo 679/2016 del Parlamento Europeo e del Consiglio, sono conformi alle previsioni del D.Lgs. 196/2003 e s.m.i. della Repubblica Italiana, al Provvedimento del Garante per la protezione dei dati n. 229 del 8 maggio 2014, nonché alla Direttiva 2002/58/CE del Parlamento Europeo e del Consiglio.

Le presenti informazioni sono in vigore dalla data di pubblicazione sul sito, ossia il 25 maggio 2018.

Cosa sono i Cookie?

I cookies sono dati creati da un server che sono memorizzati in file di testo sull'hard disk del Suo computer e consentono il funzionamento del presente sito internet, l'uso di una specifica funzionalità esplicitamente richiesta dall'utente, ovvero permettono di migliorare il funzionamento di questo sito, come i cookie che rendono la navigazione più veloce o che mostrano i contenuti di maggiore interesse per l'utente in funzione delle scelte precedenti. I cookies possono essere permanenti (c.d. cookies persistenti), ma possono anche avere una durata limitata (c.d. cookies di sessione). Questo sito utilizza sia cookies persistenti che di sessione. Quelli di sessione non vengono memorizzati in modo permanente sul Suo computer e svaniscono con la chiusura del browser. Quelli persistenti servono per personalizzare la navigazione in funzione dello strumento utilizzato dall'utente (computer, tablet, smartphone) così come i cookies di terze parti che servono per analizzare gli accessi del sito (es. Google Analytics) e per permettere agli utenti di condividere i contenuti del sito attraverso social network (FB) od e-mail (Add This). Questi cookies, vengono memorizzati in modo permanente sul Suo computer e hanno una durata variabile.

Tipologie di Cookie

La legislazione italiana (art. 122 del D.Lgs. 196/03 "Codice in materia di protezione dei dati personali" di seguito brevemente "Codice") ha introdotto nel nostro ordinamento la Direttiva Comunitaria 2009/136/CE che impone ai gestori dei siti web che utilizzano cookie o altre tecnologie di monitoraggio di informare l'utente circa le tipologie di eventuali cookie utilizzati dal sito.

Il Provvedimento del Garante per la protezione dei dati personali n. 229 del 8 maggio 2014, pubblicato sulla G.U. n. 126 del 3 giugno 2014, ha categorizzato i cookie in due macro-categorie: cookie "tecnici" e cookie "di profilazione".

Cookie Tecnici, normalmente installati dal titolare o dal gestore del sito web, hanno lo scopo di "effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente a erogare tale servizio" (cfr. art. 122, comma 1, del Codice Privacy).

Per l'installazione dei Cookie Tecnici non è richiesto il preventivo consenso degli utenti.

I cookie tecnici si suddividono ulteriormente in:

Cookie di navigazione o di sessione, che garantiscono la normale navigazione e fruizione del sito web, permettendo, ad esempio, di realizzare un acquisto o di autenticarsi per accedere ad aree riservate. Tali cookie non vengono memorizzati in modo persistente sul dispositivo utilizzato dall'utente e si disattivano automaticamente alla chiusura del browser. Il loro utilizzo è legato alla trasmissione di dati identificativi necessari per consentire una navigazione sicura ed efficiente sulle pagine. I cookie di sessione non permettono in alcun modo l'acquisizione di dati personali identificativi dell'utente.

Cookie analytics, utilizzati per raccogliere informazioni sull'utilizzo del sito, in forma anonima e per ottenere sia un'analisi statistica delle pagine visualizzate sia dei comportamenti tenuti dagli utenti. Questa analisi anonima fornisce informazioni e suggerimenti per migliorare la qualità del sito e per rendere facilmente accessibili i contenuti che si dimostrano più ricercati e interessanti agli occhi degli utenti. I cookie analytics possono essere inviati sia dal sito, sia da domini di terze parti e non permettono in alcun modo l'acquisizione di dati personali identificativi dell'utente. I cookie analytics, se installati da terze parti (es. Google analytics), anche se raccolgono i dati in forma anonima, sono assimilati ai cookie di profilazione, come indicato dal Garante per la protezione dei dati personali.

Cookie di funzionalità: assimilati ai cookie tecnici laddove utilizzati direttamente dal gestore del sito per raccogliere informazioni, in forma aggregata, sul numero degli utenti e su come questi visitano il sito stesso. Tali cookie permettono all'utente la navigazione in funzione di una serie di criteri selezionati (ad esempio, la lingua) al fine di migliorare il servizio reso allo stesso.

Cookie di Profilazione, hanno lo scopo di creare i profili dell'utente e vengono utilizzati per inviare messaggi pubblicitari in linea con le preferenze manifestate dallo stesso nell'ambito della navigazione in rete. Tali cookie sono particolarmente invasivi nella sfera privata dell'utente, per tale motivo la normativa europea e italiana prevede che l'utente debba essere adeguatamente informato sull'uso degli stessi, potendo esprimere così il proprio consenso. A essi si riferisce l'art. 122 del Codice Privacy laddove prevede che "l'archiviazione delle informazioni nell'apparecchio terminale di un contraente o di un utente o l'accesso a informazioni già archiviate sono consentiti unicamente a condizione che il contraente o l'utente abbia espresso il proprio consenso dopo essere stato informato con le modalità semplificate di cui all'articolo 13 Codice Privacy, comma 3" (art. 122, comma 1, del Codice).

Nel medesimo Provvedimento il Garante ha inoltre categorizzato i cookie a seconda del soggetto che opera in qualità di titolare del trattamento dei dati personali raccolti dal cookie, distinguendo fra cookie "di prima parte" e cookie "di terza parte".

Cookie di prima parte

Sono i cookie gestiti dal titolare del sito. Per questi cookie, l'obbligo dell'informativa spetta al titolare del sito. Spetta anche a quest'ultimo l'obbligo di indicare le modalità per l'eventuale blocco del cookie.

Cookie di terza parte

Sono i cookie gestiti da un soggetto terzo diverso dal titolare del sito. Per questi cookie, l'obbligo dell'informativa e dell'indicazione delle modalità per l'eventuale blocco del cookie spetta alla terza parte, mentre al titolare del sito è fatto obbligo di inserire nel sito il link al sito della terza parte ove tali elementi sono disponibili.

In entrambe le tipologie di cookie (di prima parte o di terza parte) la raccolta del consenso, necessario qualora il cookie sia un cookie di profilazione, avviene tramite apposito banner nella home page del sito.

Tipologie di cookie utilizzati nel nostro sito web

Il sito web **www.spesgioia.it** utilizza cookies tecnici, che possono essere utilizzati senza chiedere il consenso dell'Interessato, poiché sono strettamente necessari per la fornitura del servizio. Inoltre possono essere utilizzati cookie di profilazione di terze parti il cui utilizzo è subordinato al consenso direttamente reso a tali terze parti accedendo alle relative informative sull'uso dei cookies. I cookies di profilazione possono essere utilizzati, dal Titolare del trattamento o dal proprietario del cookie stesso, per memorizzare le scelte effettuate dall'Interessato, per fornire funzionalità personalizzate od ottimizzate o per memorizzare le sue abitudini e preferenze manifestate durante la navigazione. Ad esempio, i cookies di profilazione possono essere utilizzati per offrire all'Interessato servizi online, per inviargli pubblicità che tenga conto dei suoi interessi o per evitare che gli vengano offerti servizi che ha rifiutato in passato.

Nella sezione successiva di questa Cookie Policy è riportato in dettaglio l'elenco di tutti i cookie utilizzati da questo sito web.

Nel primo gruppo sono elencati i cookie cosiddetti tecnici il cui utilizzo non richiede il consenso dell'utente.

Nel secondo gruppo sono elencati i cookie di profilazione.

Per entrambi i gruppi, sono riportate le seguenti informazioni per ciascun tipo di cookie:

- nome del cookie
- funzione esplicata dal cookie
- indicazione se il cookie è di prima parte o di terza parte
- se il cookie è di terza parte, indicazione del link mediante il quale è possibile raggiungere il sito della terza parte ove è riportata l'informativa della terza parte stessa circa il trattamento effettuato sui dati personali raccolti tramite il cookie e sono riportate le modalità per il blocco del cookie
- scadenza del cookie.

Il sito **www.spesgioia.it** utilizza i seguenti cookies:

Cookie tecnici				
Nome cookies	**Funzione**	**Scadenza (o di sessione)**	**Prima o terza parte**	**Per i cookies di terza parte è presente il link alla cookie policy della terza parte stessa.**
_icl_current_language	**Cambio della lingua utente**	**24 ore**	**prima**	
privacy	**Conferma Accettazione privacy policy**	**7 giorni**	**prima**	
wpml_referer_url	**Gestione multiligua del sito**	**24 ore**	**prima**	
fr	**Encrypted Facebook ID and Browser ID**	**3 mesi**	**Terza**	**Privacy Policy e Cookie Policy:** https://it-it.facebook.com/privacy/explanation
CONSENT	**Utilizzato per il consenso dei**	**20 anni**	**Terza**	**Privacy e Cookie Policy:** https://policies.google.com/privacy

	servizi di Google			

Cookie di profilazione				
Nome cookies	**Funzione**	**Scadenza (o di sessione)**	**Prima o terza parte**	**Per i cookies di terza parte è presente il link alla cookie policy della terza parte stessa.**
1P_JAR	Memorizza le preferenze e le informazioni dell'utente ogni volta che visita pagine web contenenti mappe geografiche di Google Maps	1 mese	Terza	Privacy e Cookie Policy: https://policies.google.com/privacy
NID	Memorizza le preferenze e le informazioni dell'utente ogni volta che visita pagine web contenenti mappe geografiche di Google Maps	1 anno	Terza	Privacy e Cookie Policy: https://policies.google.com/privacy
_ga	Traccia i comportamenti dell'utente visitatore e traccia statistiche in Google Analytics	2 anni	Terza	Privacy e Cookie Policy: https://policies.google.com/privacy
_gat_UA-39944844-1	Traccia i comportamenti dell'utente visitatore e traccia statistiche in Google Analytics	Immediata, a chiusura del browser	Terza	Privacy e Cookie Policy: https://policies.google.com/privacy
_gid	Traccia i comportamenti dell'utente visitatore e traccia statistiche in Google Analytics	1 anno	Terza	Privacy e Cookie Policy: https://policies.google.com/privacy
IDE	Tracciamento per AdWords	1 anno	Terza	Privacy e Cookie Policy: https://policies.google.com/privacy

Non si effettuano scambi di cookie con siti esterni o fornitori esterni di dati.
L'autorizzazione alla raccolta e all'archiviazione dei dati mediante cookies può essere revocata in qualsiasi momento: l'*Interessato* può disattivare l'utilizzo dei cookies attraverso le specifiche opzioni di impostazione dei diversi browser.

- Microsoft Explorer:
https://support.microsoft.com/it-it/help/17442/windows-internet-explorer-delete-manage-cookies
- Google Chrome: https://support.google.com/accounts/answer/61416?co=GENIE.Platform%3DDesktop&hl=it
- Mozilla Firefox:
https://support.mozilla.org/it/kb/Bloccare%20i%20cookie
- Apple Safari:
https://support.apple.com/kb/ph21411?locale=it_IT

Google Analytics Cookies

Il nostro sito utilizza Google Analytics di Google, Inc., un servizio offre statistiche di misurazione ed analisi delle performance del sito, tramite l'uso di Cookie. Per consultare le informazioni privacy del servizio Google Analytics, visiti la pagina http://www.google.com/intl/en/analytics/privacyoverview.html. Per le norme sulla privacy di Google, segnaliamo il seguente indirizzo http://www.google.com/intl/it/privacy/privacy-policy.html.)

Google Adwords & Google Remarketing Cookies

Il sito internet potrebbe utilizzare il programma Google Adwords e la tecnologia Google Remarketing. Entrambi sono gestiti da Google Inc.. Anche la funzione monitoraggio delle conversioni di AdWords utilizza i cookie. Per aiutarci a monitorare le attività, viene aggiunto un cookie al computer di un utente nel momento in cui quell'utente fa clic su un

annuncio. Questo cookie dura 30 giorni e non raccoglie, né monitora informazioni in grado di identificare personalmente un utente. Gli utenti possono disabilitare i cookie del monitoraggio delle conversioni di Google nelle impostazioni del proprio browser Internet. In alcuni casi i cookie possono causare problemi al momento dell'accesso o durante la navigazione all'interno del tuo account AdWords. Quando ciò si verifica, il modo migliore per correggere il problema consiste nello svuotare la cache ed eliminare i cookie salvati per il tuo browser.
L'utente, infine, può disabilitare i cookies di Google Analytics scaricando uno specifico plug-in del browser reperibile al seguente url https://tools.google.com/dlpage/gaoptout.

Facebook Cookies

Il sito potrebbe utilizzare cookie di Facebook Inc. per monitorare l'andamento delle campagne Facebook Ads ed eventuali azioni di remarketing. Clicca qui per maggiori informazioni riguardo l'utilizzo di cookie da parte di Facebook: https://www.facebook.com/help/cookies/
L'utente può opporsi alla registrazione di cookies persistenti sul Suo hard disk configurando il browser di navigazione in modo da disabilitare i cookies. Scopri come disabilitare i cookie nei principali browser: Chrome, Firefox, Internet Explorer, Safari, Opera. Dopo questa operazione, tuttavia, alcune funzioni delle pagine web potrebbero non essere eseguite correttamente.

PER QUALI FINI SONO TRATTATI I DATI?

I dati raccolti dal *Titolare del trattamento* sono utilizzati al fine di:

- contare il numero dei visitatori del sito;
- controllare se Lei ha operato attraverso e-mail o attraverso un link;
- verificare quanto sia stata di successo una specifica campagna pubblicitaria;
- stabilire particolari livelli di interesse per particolari sezioni o aspetti del sito o per particolari prodotti e servizi disponibili su questo sito;
- capire quanto sia popolare un prodotto o un servizio e il livello di variazione dell'interesse tra i particolari prodotti e i servizi del titolare;
- migliorare l'utilizzo del sito e registrare statistiche sul suo utilizzo, oltre che profilare gli *Interessati*;

registrare e censire l'*Interessato* sul sito web **www.spesgioia.it.**

- inviare comunicazioni di carattere commerciale riguardanti l'attività svolta e i servizi offerti dalla società **Servizi polifunzionali ecosostenibili Gioia s.p.a.**

I dati potranno essere trattati anche mediante processi decisionali automatizzati, quali ad esempio la profilazione, al fine di migliorare la navigazione e l'offerta al cliente.

AGGIORNAMENTO DELLA PRESENTE COOKIE POLICY

La presente Cookie Policy è stata aggiornata in data 11 ottobre 2018. Eventuali aggiornamenti saranno sempre pubblicati in questa pagina.
Per ulteriori informazioni sulla privacy clicca qui.