Procedure al 30/11/2023

Nella presente sezione, aggiornata ad ogni variazione, sono collezionate le procedure quali strumenti di supporto per adempiere agli obblighi e a dar evidenza degli adempimenti relativi al REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (regolamento generale sulla protezione dei dati - GDPR) nell'ambito delle attività svolte.

INSIT INDUSTRIA SPA

Identificativo nazionale (C.F.): 00937240042

Luogo, Data Torino, 30/11/23

Firma

SIG.RA DEBENEDETTI ANNA

Dott.ssa Anna Debenedetti
DIRETTORE GENERALE
INSIT INDUSTRIA SPA

Pagina intenzionalmente vuota

Sommario

Procedura per il monitoraggio e la gestione delle violazioni di dati (data breach)

La presente procedura ha lo scopo di descrivere le attività che INSIT INDUSTRIA SPA deve porre in essere per gestire gli incidenti e le violazioni dei dati personali ai sensi degli artt. 33-34 del Regolamento (UE) 2016/679.

Responsabilità

La responsabilità di tale attività ricade su:

- Delegato Privacy per la protezione dei dati;
- DPO, ove designato;
- Preposto alla gestione dei sistemi ICT, ove designato;
- Eventuali responsabili del trattamento, se richiesto loro nelle istruzioni;
- Eventuali ulteriori amministratori di sistema, ove designati;

Ambito di applicazione

Per Data Breach (o "Violazione dei dati personali") si intende un incidente di sicurezza, per effetto del quale, non si è in grado di garantire il rispetto dei principi prescritti dall'art. 5 del GDPR per il trattamento dei dati personali, che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (Art. 4 p.12 GDPR).

Si possono distinguere tre tipi di violazioni, che potrebbero essere combinate tra loro:

- Violazione di riservatezza, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale.
- Violazione di integrità, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale.
- Violazione di disponibilità, ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.

Sono dunque monitorati e considerati i seguenti eventi:

- distruzione, perdita, alterazione, anche accidentali,
- archiviazione, trattamento, accesso o divulgazione non autorizzati o illeciti.

Solitamente il Data Breach si realizza con una divulgazione di dati personali all'interno di un ambiente

privo di misure di sicurezze (da esempio, su web) in maniera involontaria o volontaria, ad esempio, quando i dati personali sono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato. Tale divulgazione potrebbe avvenire, ad esempio in seguito a:

- *perdita accidentale: ad esempio, Data Breach causato da smarrimento di una chiavetta USB contenente dati riservati;*
- *furto: ad esempio, Data Breach causato da furto di un notebook contenente dati confidenziali;*
- *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.*

Verifica di efficacia della procedura

L'efficacia della presente procedura verrà valutata mediante audit annuale effettuato a volto a verificare la correttezza dello svolgimento della procedura.

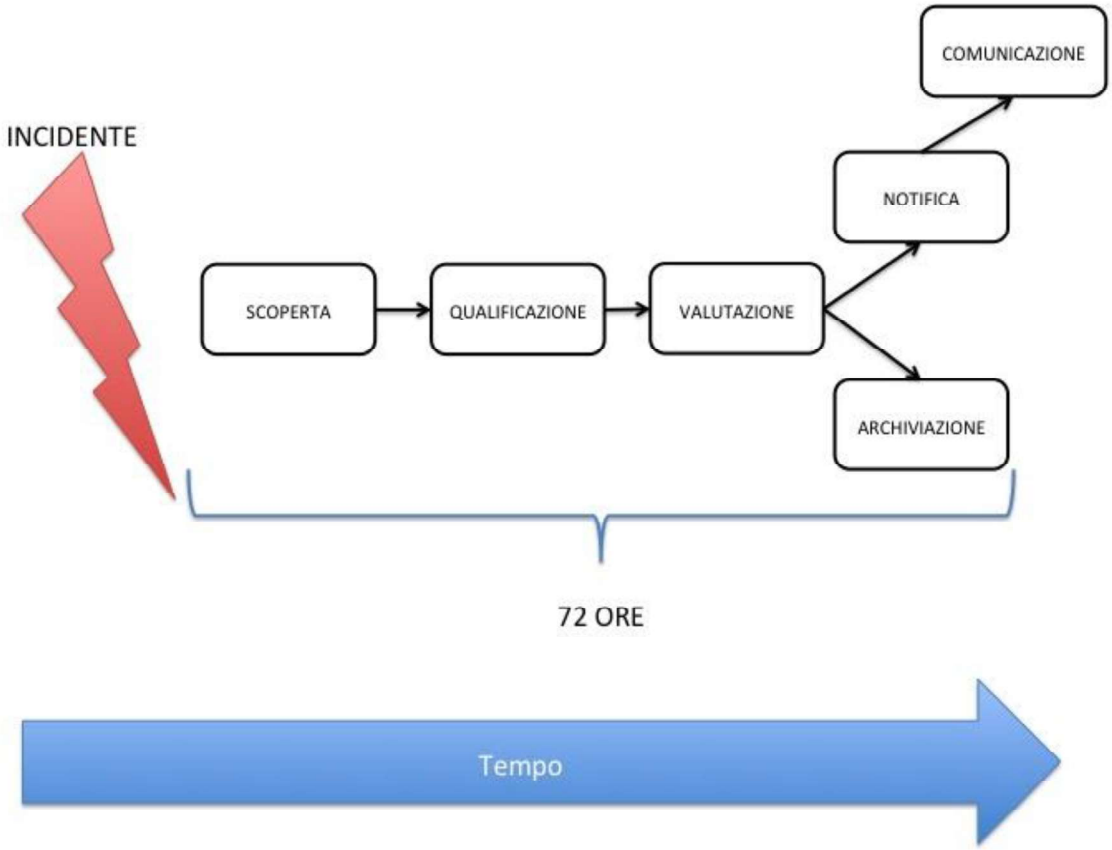
Criteri applicabili

Le segnalazioni circa gli incidenti che potrebbero sfociare in un Data Breach:

- Sono fatte dagli autorizzati e responsabili al Delegato Privacy;
- Sono fatte dagli interessati e da terzi al punto di contatto privacy presidiato;
- Derivano dai sistemi di monitoraggio automatici dei sistemi informatici (in quanto la responsabilità è anche commisurata secondo la capacità di scoprire tempestivamente un incidente ed indagarlo).

Ricevuta la segnalazione il Delegato Privacy deve identificare l'incidente di sicurezza, comprendere se l'incidente ha impatto sulle informazioni e, infine, determinare se tra le informazioni coinvolte dall'incidente vi sono dati personali. L'obbligo di notificazione al Garante (entro 72 dalla scoperta) e quello aggiuntivo di comunicazione agli interessati coinvolti devono essere valutati caso per caso in relazione ai diritti ed alla libertà degli interessati e tenuto conto che, in particolare per tale seconda comunicazione non è dovuta se il rischio per gli interessati non è elevato o se si utilizzano (e lo si può dimostrare) misure, come ad es. la cifratura, che rendono i dati inintelligibili a chiunque non sia autorizzato ad accedervi e che tali misure erano state applicate al momento della violazione.

Le attività di scoperta dell'incidente e quelle successive di gestione sono documentate adeguatamente (devono riportare le violazioni, le circostanze, le conseguenze ed i rimedi), tracciabili, replicabili ed essere in grado di fornire evidenza nelle sedi competenti, al fine di consentire all'autorità di controllo di verificare il rispetto della norma.



Ogni violazione dei dati personali è annotata nel **Registro delle Violazioni dei Dati** (acronimo **RVD**) e contiene:

- la data in cui è annotata;
- la data della sua scoperta;
- le circostanze a essa relative;
- 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;
- le conseguenze ipotizzate all'atto della scoperta;
- le misure e i provvedimenti adottati e da adottare per porvi rimedio e anche, se del caso, per attenuarne i possibili effetti negativi, indicando tempistiche e soggetti preposti al loro assolvimento;
- la valutazione dei rischi per i diritti e le libertà delle persone fisiche relativamente alla violazione in questione, con l'indicazione della necessità o meno di provvedere alla notificazione ai sensi dell'art. 33 del GDPR all'Autorità di controllo e/o alle comunicazioni ai sensi dell'art. 34 del GDPR agli interessati;
- il riferimento alla notificazione ai sensi dell'art. 33 del GDPR all'Autorità di controllo, gestita secondo le corrette modalità di comunicazione, dettagliando anche il momento e il mezzo del suo invio;
- il riferimento alle comunicazioni ai sensi dell'art. 34 del GDPR agli interessati, gestita secondo le corrette modalità per le comunicazioni, dettagliando anche il momento e il mezzo del suo invio;

- uno o più riesami con l'indicazione dell'evoluzione delle conseguenze della violazione fino alla sua chiusura; i riesami contengono la data in cui esso avviene, le conseguenze realizzatesi a causa della violazione, la valutazione circa i provvedimenti adottati, l'aggiornamento delle indicazioni in merito ai provvedimenti da adottare.

Descrizione processo e definizione dei compiti

Qualora il personale interno (lavoratori, collaboratori, autorizzati, preposti, responsabili, ecc.) dovesse rilevare che si è verificato un Data Breach ovvero che vi è un rischio serio ed imminente di violazione dei dati personali detenuti, dovrà seguire la procedura di seguito descritta, con la massima puntualità ed efficienza.

Scoperta

La scoperta di un incidente di sicurezza può essere svolta da diversi attori, interni e/o esterni all'organizzazione:

- dagli autorizzati (personale dipendente, convenzionato, stagisti, tirocinanti, ecc)
- da parte dei Responsabili esterni del trattamento
- da parte del DPO (ove designato)
- da parte degli organi Pubblici (Agid, Polizia, altre Forze dell'Ordine, giornalisti, ecc)
- dai sistemi di monitoraggio automatici dei sistemi informatici
- dagli interessati e da terzi

Esempi

- *Violazioni del sistema informatico*
- *Hackeraggio*
- *Perdita di dispositivi aziendali*
- *Attivazione di Cryptolocker*
- *Accesso non autorizzato ad archivi cartacei.*

è opportuno che l'attore attivi una pronta risposta per contrastare la minaccia che dipende da caso a caso.

Esempi
Nel caso di incidente informatico legato a malware:

- *scollegare il terminale dalla rete ethernet e/o disattivare wi-fi*
- *attivare il software antivirus e far eseguire un ciclo di analisi*

In ogni caso, il soggetto che prende coscienza dell'incidente di sicurezza: informa tempestivamente il Delegato Privacy **SIG.RA DEBENEDETTI ANNA** e, laddove designato, anche il Responsabile della Protezione dei Dati (o DPO - Data Protection Officer), inviando opportuna segnalazione mediante messaggio di posta elettronica al punto di contatto privacy presidiato (**INFO@INSITINDUSTRIA.COM**) e in copia direttamente all'indirizzo lavorativo personale e mediante avvertimento verbale/telefonico in ogni caso.

Il Delegato Privacy, dal momento in cui viene a conoscenza dell'evento, procede alla fase successiva di qualificazione dell'incidente.

Qualificazione dell'incidente

Se l'incidente di sicurezza ha impatto (a qualunque livello) su informazioni (documenti, file, strumenti, servizi, ecc.) contenenti dati personali allora si tratta di una violazione di dati e va valutata (fase di valutazione dell'impatto della violazione) per determinare tipologia e quantità dei dati personali oggetto del data breach e individuare contromisure tecniche correttive e preventive; altrimenti l'incidente non deve essere preso in considerazione ai fini della presente procedura.

Ogni violazione dei dati personali è dunque annotata (art. 33 p.5 GDPR) nel **Registro delle Violazioni dei Dati** (**RVD**), come specificato sopra.

Le annotazioni nel RVD garantiscono che sia dimostrabile il momento della scoperta dell'incidente, poiché da quel momento decorrono le 72 ore per la notificazione, il cui scopo è di limitare i danni che possono derivare per effetto di una violazione a carico degli interessati, fatto che dipende dalla tempestività e dall'adeguatezza con cui la violazione è affrontata. La comunicazione invece risponde allo scopo di consentire all'interessato, qualora sussista una violazione che presenta rischi elevati, di prendere le precauzioni necessarie.

Contenimento e adozione di contromisure

Contestualmente alla qualificazione occorre continuare a perseguire le misure per bloccare e contenere le conseguenze dannose dell'incidente, iniziate nella fase di scoperta, coinvolgendo altri soggetti (es. preposto ICT, amministratori di sistema, ecc.).

Valutazione dell'impatto della violazione

Nel determinare l'obbligo di notificazione e di successiva comunicazione occorre valutare la possibilità che la violazione possa causare danni fisici, materiali o immateriali alla persona fisica, quali ad esempio (Considerando 85 GDPR):

- perdita del controllo dei dati personali degli interessati;
- limitazione dei diritti;
- discriminazione;
- furto o usurpazione di identità;
- perdite finanziarie;
- decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale, o qualsiasi altro danno economico o sociale significativo per la persona interessata.

Nel dettaglio si applica la metodologia sviluppata dall'ENISA (European Union Agency for Network and Information Security) pubblicata nel dicembre 2013, riportata in allegato nelle parti fondamentali per definire se il Data Breach verificatosi possa comportare un rischio per i diritti e le libertà delle persone fisiche i cui dati personali sono stati violati e se, conseguentemente debbano essere fatte le comunicazioni di cui agli Artt. 33 e/o 34 del GDPR al Garante ed agli interessati.

Per tale valutazione sono utilizzate le informazioni riportate in fase di scoperta, di contenimento e adozione delle contromisure. Se necessario, si consultano i legali per acquisire un parere in proposito.

Trattamento svolto come responsabile

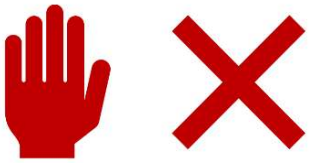
Quando il trattamento oggetto della violazione è svolto in qualità di responsabile o sub-responsabile per conto del Titolare del trattamento, a cui spetta l'obbligo di notificazione a meno di diverse pattuizioni contrattuali, vige il dovere di:

- informare tale Titolare senza ingiustificato ritardo quando si viene a conoscenza di una violazione e
- supportarlo nel valutare la portata di questo in termini di impatto rispetto ai dati personali ed ai diritti e la libertà degli interessati.

Trattamento svolto come titolare

Se NON SUSSISTE il rischio per i diritti e le libertà delle persone fisiche i cui dati personali sono stati violati

Si redige decisione scritta e motivata in merito alla valutazione di assenza di rischio e di non effettuare le comunicazioni di cui agli Artt. 33 e/o 34 del GDPR al Garante ed agli interessati, annotandola nel RVD. Allega alla stessa tutti i documenti, pareri, rapporti acquisiti.



Se SUSSISTE il rischio per i diritti e le libertà delle persone fisiche i cui dati personali sono stati violati

Si procede alla notificazione (art.33 del GDPR) al Garante tramite apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/ (si veda: Provvedimento del 27 maggio 2021).[1]

- Nella stessa pagina è disponibile un modello facsimile, da NON utilizzare per la notifica al Garante ma utile per vedere in anteprima i contenuti che andranno comunicati al Garante e le **Istruzioni per l'utilizzo della procedura telematica**.
- Per semplificare gli adempimenti previsti per il Titolari del trattamento, il Garante ha ideato e messo disposizione un apposito strumento di autovalutazione (self assessment) che consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza.

Se il rischio è **ELEVATO**, si procede alla comunicazione anche agli interessati (art.34 del GDPR), via e-mail, sms o a mezzo posta sulla base del *formulario CI.*

[1] A partire dal 1° luglio 2021, la notifica di una violazione di dati personali non avviene più mediante invio per mezzo di PEC del Modello di notifica "Formulario NG".

Formulario CI (comunicazione all'interessato)

Oggetto: comunicazione ai sensi dell'Art. 34 del Regolamento Generale sulla Protezione dei Dati personali

Gentile Signora / Egregio Signore,
Siamo spiacenti di informarLa che, a causa di:

- un problema tecnico dei nostri sistemi informatici
- un accesso non autorizzato alle nostre banche dati digitali / cartacee
- la perdita di un archivio digitale o cartaceo

si è verificata / potrebbe essersi verificata una violazione dei Suoi dati personali trattati dalla nostra azienda.
Per qualsiasi informazione in proposito, può rivolgersi al nostro servizio di assistenza scrivendo una e-mail all'indirizzo e-mail ..... oppure chiamando i nostri operatori al numero +39 .....
Le probabili conseguenze della violazione dei Suoi dati personali potrebbero essere:

_____
_____
_____
_____
_____

Al fine di porre rimedio alla violazione e per attenuarne i possibili effetti negativi, la nostra azienda ha adottato le seguenti misure:

_____
_____
_____
_____
_____

Distinti saluti,

Inintelligibilità dei dati.

A giudizio dell'Autorità per Protezione dei Dati[2], si considerano inintelligibili i dati che, ad esempio:

- siano stati cifrati in modo sicuro attraverso un algoritmo standardizzato, o mediante l´impiego di schemi di cifratura a chiave simmetrica o pubblica noti in letteratura, purché la chiave di decifrazione sia di adeguata lunghezza (espressa in numero di bit), sia stata predisposta dal titolare una policy per la relativa custodia, e se essa non sia stata compromessa da violazioni della sicurezza e sia stata generata in modo da non consentirne la derivazione con gli strumenti tecnologici disponibili da parte di soggetti non autorizzati ad accedervi; oppure
- siano stati sostituiti da un valore di hash calcolato attraverso una funzione crittografica di hashing a chiave, purché la chiave utilizzata per effettuare lo hashing dei dati sia di adeguata lunghezza

[2] Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. data breach) - 4 aprile 2013 (Pubblicato sulla Gazzetta Ufficiale n. 97 del 26 aprile 2013), Registro dei provvedimenti n. 161

(espressa in numero di bit), sia stata predisposta dal titolare una policy per la relativa custodia, e se essa non sia stata compromessa da violazioni della sicurezza e sia stata generata in modo da non consentirne la derivazione con gli strumenti tecnologici disponibili da parte di soggetti non autorizzati ad accedervi; oppure

● siano stati resi anonimi con procedure tali da non consentire la reidentificazione degli interessati cui si riferiscono da parte di soggetti non legittimati al loro trattamento, anche mediante il ricorso ad altre fonti informative disponibili presso il titolare o pubbliche.

Metodologia di valutazione di impatto ENISA - dicembre 2013

Metodologia di valutazione di impatto ENISA - dicembre 2013

Criteri

I principali criteri presi in considerazione durante la valutazione dell'impatto di una violazione dei dati personali sono:

- Contesto dell'elaborazione dei dati {DPC – Data Procesing Context}: applicabile al tipo di dati violati, insieme a una serie di fattori collegati al contesto generale dell'elaborazione.
- Facilità di identificazione (El – Ease of identification): determina il grado di facilità nell'individuazione dell'identità degli individui coinvolti nella violazione (più bassa è la facilità di identificazione, più basso sarà il coefficiente applicabile) può essere dedotta dai dati coinvolti nella violazione.
- Circostanze di violazione (CB – Circumstances of breach): quantifica le specifiche circostanze della violazione classificate secondo tre tipologie di *breach* (perdita di riservatezza, integrità e disponibilità), inclusa la perdita di sicurezza dei dati violati, nonché qualsiasi intento malevolo coinvolto.

Valutazione di impatto

In base ai criteri di cui sopra, l'approccio di questa metodologia è il seguente:

- Il DPC è al centro della metodologia e valuta la criticità di una serie di dati in un contesto di elaborazione specifico. Tale fattore inerisce alle tipologie dei dati coinvolti (dati comuni, giudiziari, particolari e sensibili), tanto più sarà "sensibile" il dato colpito dal breach tanto più sarà elevato il coefficiente correlato a questo fattore.
- Fattore correttivo EI del DPC. La criticità complessiva di un trattamento dei dati può essere ridotta a seconda del valore di El. In altri termini, minore è il caso dell'identificazione, minore è il punteggio complessivo. Pertanto, la combinazione di El e DPC (moltiplicazione) fornisce il punteggio iniziale dell'impatto (SE) della violazione dei dati.
- CB quantifica le specifiche circostanze della violazione che possono essere presenti o meno in una particolare situazione. Quindi, quando è presente, CB può solo incrementare l'impatto di una specifica violazione. Per questo motivo, il punteggio iniziale può essere ulteriormente influenzato dal CB.

Definizione del livello di impatto

Come introdotto nella Sezione 2.2, l'impatto complessivo (SE - the overall severity) è calcolato con la seguente formula:

SE = DPC x EI + CB

Il punteggio finale mostra il livello dell'impatto di una determinata violazione, tenendo conto dell'impatto sugli individui.

		Impatto di una violazione dei dati (Data Breach)
SE < 2	Basso	Gli individui possono andare incontro a disagi minori, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.)
2 < SE < 3	Medio	Gli individui possono andare incontro a significativi disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.).
3 < SE< 4	Alto	Gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).
SE > 4	Molto alto	Gli individui possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).

Indicatori

Una volta definito il livello di severità dell'impatto, è possibile utilizzare dagli indicatori che segnalano alcuni elementi della violazione che, sebbene non influenzino a priori il punteggio, sono importanti per la valutazione finale. Ai fini della metodologia, sono stati considerati due indicatori:

- Il numero di persone violate supera le 100 unità. I dati di un individuo, violati in un incidente di ampio contesto, possono potenzialmente essere più facilmente rivelati, mentre allo stesso tempo un numero elevato di individui colpiti, influenza la scala complessiva della violazione.
- Dati incomprensibili. L'incomprensibilità (ad esempio sotto forma di crittografia forte e senza compromissione della chiave) può ridurre sostanzialmente l'impatto sugli individui, poiché riduce notevolmente la possibilità che soggetti non autorizzati accedano ai dati.

Allegato 1 - Contesto dell'elaborazione dei dati

A1_Tabella di Valutazione

Tabella 1: Contesto elaborazione dati (DPC - Data Processing Context)		Score
Dati semplici	Per esempio. dati biografici, dati di contatto, nome completo, dati sull'istruzione, vita familiare, esperienza professionale, ecc.	
	Punteggio di base preliminare: quando la violazione riguarda "dati semplici" e il Titolare del trattamento non è a conoscenza o fattori aggravanti.	1
	Il punteggio DPC potrebbe essere aumentato di 1, ad es. quando il volume o/i dati semplici e/o le caratteristiche o il Titolare del trattamento sono tali da consentire l'abilitazione di determinati profili o dell'individuo o presupposti relativi allo stato sociale/finanziario dell'individuo.	2
	Il punteggio DPC potrebbe essere incrementato di 2, ad es. quando i "dati semplici" e/o le caratteristiche del Titolare del trattamento possono portare a supposizioni sullo stato di salute dell'individuo, sulle preferenze sessuali, sulle convinzioni politiche o religiose.	3
	Il punteggio DPC potrebbe essere aumentato di 3, ad es. quando a causa di determinate caratteristiche dell'individuo (ad es. gruppi vulnerabili, minori), l'informazione può essere critica per la sicurezza personale o per le condizioni fisiche/psicologiche.	4
Dati comportamentali	Per esempio. posizione, dati sul traffico, dati su preferenze personali e abitudini, ecc.	
	Punteggio di base preliminare: quando la violazione riguarda "dati comportamentali" e i Titolari del trattamento non sono a conoscenza di fattori aggravanti o di diminuzione.	2
	Il punteggio DPC potrebbe essere diminuito di 1, ad es. quando la natura del set di dati non fornisce alcuna comprensione sostanziale delle informazioni comportamentali dell'individuo o i dati possono essere raccolti facilmente (indipendentemente dalla violazione) attraverso fonti disponibili pubblicamente (ad esempio combinazione di informazioni da ricerche web).	1
	Il punteggio DPC può essere aumentato di 1, ad es. quando il volume di "dati comportamentali e/o le caratteristiche del Titolare del trattamento sono tali da consentire la creazione di un profilo individuale, esponendo informazioni dettagliate sulla sua vita quotidiana e sulle sue abitudini.	3
	Il punteggio DPC può essere aumentato di 2, ad es. se è possibile creare un profilo basato sui dati sensibili di una persona.	4
Dati finanziari	Qualsiasi tipo di dati finanziari (ad es. Reddito, transazioni finanziarie, estratti conto bancari, investimenti, carte di credito, fatture, ecc.). Include dati sul benessere sociale relativi alle informazioni finanziarie.	
	Punteggio di base preliminare: quando la violazione riguarda "dati finanziari" e il Titolare del trattamento non è a conoscenza di fattori aggravanti o di diminuzione.	3
	Il punteggio DPC potrebbe essere ridotto di 2, ad es. quando la natura del set di dati non fornisce alcuna comprensione sostanziale delle informazioni finanziarie dell'individuo (ad esempio il fatto che una persona sia il cliente di una determinata banca senza ulteriori dettagli).	1
	Il punteggio DPC potrebbe essere diminuito di 1, ad es. quando il set di dati specifici include alcune informazioni finanziarie ma non fornisce ancora informazioni significative sullo stato / sulla situazione finanziaria dell'individuo (ad esempio numeri di conti bancari semplici senza ulteriori dettagli).	2

	Il punteggio DPC potrebbe essere aumentato di 1, ad es. quando a causa della natura e/o del volume dell'insieme di dati specifico, vengono divulgate informazioni finanziarie complete (ad esempio carta di credito) che potrebbero consentire di frodare o creare un profilo sociale/finanziario dettagliato.	4
Dati sensibili	Qualsiasi tipo di dati sensibili (ad esempio salute, appartenenza politica, vita sessuale)	
	Punteggio di base preliminare: quando la violazione riguarda "dati sensibili" e il Titolare del trattamento non è a conoscenza di eventuali fattori di diminuzione.	4
	Il punteggio DPC potrebbe essere diminuito di 1, ad es. quando la natura del set di dati non fornisce alcuna comprensione sostanziale delle informazioni comportamentali dell'individuo o i dati possono essere raccolti facilmente (indipendentemente dalla violazione) attraverso fonti disponibili pubblicamente {ad es. combinazione di informazioni da ricerche web).	1
	Il punteggio DPC potrebbe essere ridotto di 2, ad es. quando la natura dei dati può portare a ipotesi generali.	2
	Il punteggio DPC potrebbe essere diminuito di 1, ad es. quando la natura dei dati può portare a supposizioni su informazioni sensibili.	3

A2_Descrizione dei fattori contestuali da considerare nel punteggio DPC

Fattori crescenti:

● Volume dei dati violati (per lo stesso individuo): questo fattore può aumentare il punteggio DPC di base, a causa dell'incremento della quantità delle informazioni violate (agendo come fattore aggravante). Il volume dovrebbe essere considerato sia in termini di tempo (ad esempio considerando lo stesso tipo di dati in un determinato periodo di tempo) che di contenuto (dati complementari dello stesso tipo). Ad esempio, in caso di violazione dei dati sul traffico presso un ISP (Internet Service Provider), il punteggio DPC sarebbe più alto (per lo stesso individuo) se i dati coprono un periodo di tempo pari ad un anno rispetto a se sono limitati ad una settimana (criterio temporale). Ulteriormente, ad esempio, in caso di violazione di una banca, il punteggio DPC del fascicolo completo di un individuo sarebbe superiore a quello di un singolo documento dello stesso fascicolo (criterio di contenuto).

● Caratteristiche speciali del Titolare: questo fattore si riferisce al campo di attività e alle attività del Titolare del trattamento dei dati, che potrebbe aumentare il punteggio DPC di base, rivelando informazioni aggiuntive per un determinato insieme di dati. Ad esempio, il punteggio DPC di una lista clienti sarebbe maggiore se proviene da una farmacia online piuttosto che da una cartoleria.

● Caratteristiche speciali degli individui: il punteggio DPC di base di un determinato insieme di dati potrebbe anche essere aumentato nel caso in cui gli individui appartengano a un gruppo sociale con bisogni particolari (ad esempio minori, individui di un particolare gruppo con caratteristiche speciali). Ad esempio, il punteggio DPC di un elenco di numeri di telefono aumenterebbe se riguardasse membri noti del parlamento nazionale.

Fattori decrescenti:

● Invalidità/inesattezza dei dati: il punteggio DPC di base di un determinato set di dati può essere ridotto se l'invalidità o l'inesattezza dei dati è nota al Titolare del trattamento (ad esempio a causa della loro età o contenuto) e, quindi, la loro importanza è minore. Il Titolare del trattamento deve essere certo di questa circostanza per includerlo nella valutazione. Ad esempio, l'elenco di indirizzi

di un servizio postale in cui le lettere non potevano essere consegnate sarebbe considerato impreciso (ad esempio, molto probabilmente gli individui si sono spostati in un altro indirizzo).

- Disponibilità pubblica: il punteggio DPC di base di un set di dati può anche essere ridotto nel caso in cui i dati violati fossero già disponibili pubblicamente prima della violazione o possano essere facilmente raccolti e/o accessibili tramite fonti disponibili pubblicamente.

- Natura dei dati: un altro fattore che diminuisce il punteggio del DPC, potrebbe in alcuni casi essere la natura stessa di un particolare set di dati che, nonostante il punteggio iniziale del DPC, è di minore importanza, in termini di informazioni che può rivelare sull'individuo. Questo è, ad esempio, il caso di un certificato medico che sta solo certificando che l'individuo è in buono stato di salute senza rivelare altre informazioni. In questo caso, sebbene il punteggio di base sarebbe 4 dato che i dati sulla salute sono dati sensibili, il punteggio DPC finale del set di dati specifici diviene 1, in quanto non può di per sé influenzare la vita personale dell'individuo. Questo fattore, tuttavia, dovrebbe essere considerato con grande cura e chiara spiegazione del motivo per cui un particolare trattamento dei dati è per sua natura inferiore al suo punteggio DPC di base.

Allegato 2 - Facilità di identificazione (EI- Ease of identification) punteggio

Questo allegato presenterà gli esempi di punteggio EI (Ease of identification) per gli identificatori comuni.

L'identificazione può essere diretta o indiretta e viene eseguita con l'uso di determinati identificatori, tenendo conto anche del contesto generale del trattamento dei dati personali. Gli esempi seguenti mostrano un elenco (non esaustivo) di identificatori comuni e diversi casi del loro possibile utilizzo per il punteggio EI (Ease of identification).

Va notato che in molti casi la violazione includerà una combinazione di diversi identificatori, che aumenta automaticamente la facilità di identificazione. Questo è un elemento molto importante che dovrebbe essere preso in considerazione dal Titolare del trattamento e si riflette negli esempi seguenti.

Nome e cognome

È considerato come l'identificatore diretto più comune, ma il punteggio EI (Ease of identification) può variare a seconda del caso, poiché il nome completo non sempre è di per sé univoco. Ad esempio, quando l'identificazione viene eseguita utilizzando solo il nome completo dell'individuo:

- EI = 0,25 (Trascurabile) in tutta la popolazione di un paese in cui molte persone condividono lo stesso nome completo.
- EI = 0,5 (Limitato) nella popolazione di un paese in cui poche persone condividono lo stesso nome completo.
- EI = 0,75 (Significativo) nella popolazione di una piccola città in cui poche o nessuna persona condivide lo stesso nome completo.
- EI = 1 (Massimo) nella popolazione di un paese utilizzando anche data di nascita e indirizzo e-mail.

Carta d'identità / passaporto / numero di previdenza sociale

Sono tutti considerati come identificatori univoci e possono essere utilizzati per individuare l'individuo, purché sia possibile collegarli a un database di riferimento (ad esempio collegando una carta d'identità a una determinata persona). Ad esempio, quando l'identificazione viene eseguita utilizzando solo uno di questi numeri:

- EI = 0,25 (Trascurabile) quando non sono fornite altre informazioni sull'individuo o non è possibile trovare ulteriori informazioni a meno che non si abbia accesso al database di riferimento.
- EI = 0,75 (Significativo) quando l'identificativo rivela ulteriori informazioni identificative sull'individuo (ad es. codice fiscale che rivela la data di nascita) ed è collegato ad altri dati (ad esempio indirizzo postale o e-mail).
- EI = 1 (Massimo) quando sono disponibili anche le informazioni dal database di riferimento (ad esempio carta d'identità e nome completo e/o immagine).

Numero di telefono / indirizzo di casa

Sono entrambi identificatori indiretti, che possono anche essere usati per comunicare o accedere all'individuo. Quando l'identificazione si basa solo su uno di questi due identificativi:

- El = 0,25 (Trascurabile) in tutta la popolazione di un paese quando il numero di telefono / indirizzo non è registrato in un registro disponibile al pubblico.
- El = 0,5 (Limitato) in tutta la popolazione di una piccola città e il numero di telefono / indirizzo non è registrato in un registro disponibile pubblicamente (identificazione possibile tramite comunicazione).
- El = 1 (Massimo) nella popolazione di un paese e il numero di telefono / indirizzo è incluso nel registro disponibile pubblicamente.

Indirizzo e-mail

È anche un identificatore indiretto, che può essere usato per comunicare con l'individuo e in alcuni casi può includere informazioni sul suo nome (nome e/o cognome). Quando l'identificazione è basata sulla posta elettronica:

- El = 0,25 (Trascurabile) quando l'indirizzo di posta elettronica non rivela altre informazioni di identificazione (ad es. Nome) e non è utilizzato come indirizzo primario dell'individuo in siti internet, forum o social network.
- El = 0,75 (Significativo) quando l'indirizzo e-mail non rivela altre informazioni di identificazione (ad esempio nome) ma viene utilizzato come indirizzo primario dell'individuo in siti internet, forum o social network (ricercabili sul Web).
- El = 1 (Massimo) quando l'indirizzo e-mail rivela il nome dell'individuo e viene utilizzato come indirizzo principale in siti internet, forum o social network (ricercabili sul web).

Immagine

Potrebbe essere un identificatore diretto o indiretto, a seconda dei casi. Ad esempio, quando l'identificazione si basa solo su un'immagine:

- El = 0,25 (Trascurabile) quando l'immagine non è chiara o vaga (ad esempio, metraggio CCTV da una lunga distanza).
- El = 05 (Limitato) quando l'immagine non è chiara o vaga, ma include informazioni aggiuntive (ad esempio dintorni che mostrano una posizione specifica) che potrebbero portare all'individuazione dell'individuo.
- El = 0,75 (Significativo) quando l'immagine è chiara ma nessun'altra informazione di identificazione è collegata ad essa.
- El = 1 (Massimo) quando l'immagine è chiara e collegata ad alcune informazioni aggiuntive (ad esempio informazioni sull'appartenenza a un gruppo specifico, indirizzo di casa, ecc.).

Codifica / Aliases / Iniziali

La codifica si riferisce all'assegnazione di un numero identificativo univoco a ciascun individuo, ad es. nel contesto di un database specifico. L'uso di alias è una forma di pseudonimizzazione, nel senso che un identificatore specifico (di solito il nome completo dell'individuo) è sostituito da un alias (pseudonimo). Le iniziali sono un tipo di alias che viene estratto dal nome completo dell'individuo. Come nel caso degli identificatori univoci, i codici e gli alias possono essere utilizzati per identificare l'individuo fintanto che è possibile collegarli a un database di riferimento (ad esempio collegando il codice / alias al nome completo di una particolare persona) Quando l'identificazione è basato sulla codifica o sull'uso di alias:

● EI = 0,25 (Trascurabile) quando il codice / alias non rivela e non può essere collegato a nessun altro dato personale sulla persona a meno che non si abbia accesso al database di riferimento.
● EI = 0,75 (Significativo) quando l'alias rivela alcuni dati sull'individuo (ad esempio, il nome) ed è collegato ad altri dati personali (ad esempio l'indirizzo e-mail dell'individuo).
● EI = 1 (Massimo) quando l'alias rivela il nome completo dell'individuo oi dati dal database di riferimento sono anche disponibili.

Allegato 3 - Esempi delle circostanze del punteggio di violazione (CB)

A1 Perdita di riservatezza

0 - Esempi di dati esposti a rischi di riservatezza senza prove che l'elaborazione illegale si è verificata.

- Un file cartaceo o un laptop si perde durante il transito.
- L'attrezzatura è stata smaltita senza distruzione dei dati personali.

+0.25 - Esempi di dati disposti per un numero di destinatari noti:

- Un'email con dati personali è stata inviata erroneamente a un certo numero di destinatari noti.
- Alcuni clienti possono accedere agli account di altri clienti in un servizio online.

+0.5 - Esempi di dati disposti a un numero sconosciuto di destinatari:

- I dati sono pubblicati su una bacheca internet.
- I dati sono caricati su un sito P2P.
- Un dipendente vende un CD ROM con i dati del cliente.
- Un sito web configurato in modo errato rende accessibili pubblicamente i dati Internet dagli utenti interni.

A2 Perdita di integrità

0 - Esempi di dati modificati ma senza alcun uso errato o illegale identificato:

- I registri di un database con dati personali sono stati erroneamente aggiornati ma è stata salvata una copia dell'originale prima che si verifichi qualsiasi utilizzo dei dati modificati.

+0.25 - Esempi di dati modificati ed eventualmente usati in modo errato o illegale ma con possibilità di recupero:

- È stato modificato un record necessario per la fornitura di un servizio sociale online e l'individuo deve richiedere il servizio in modalità offline.
- È stato modificato un record importante per l'accuratezza del file di un individuo in un servizio medico online.

+0.5 - Esempi di dati modificati ed eventualmente usati in modo errato o illegale senza possibilità di recupero:

- Gli esempi precedenti + l'originale non possono essere recuperati.

A3 Perdita di disponibilità

0 - Esempi di dati che possono essere recuperati senza difficoltà:

- Una copia del file è persa ma sono disponibili altre copie.
- Un database è corrotto ma può essere facilmente ricostruito da altri database.

+0.25 - Esempi di indisponibilità temporale:

- Un database è corrotto ma può essere ricostruito da altri database, sebbene sia richiesta qualche elaborazione.
- Un file è perso ma le informazioni possono essere fornite di nuovo dall'individuo.

+0.5 - Esempi di indisponibilità totale (i dati non possono essere recuperati dal controllore o dai singoli):

- Un file è perso / database danneggiato, non c'è il backup di queste informazioni e non può essere fornito dall'individuo.

A3 Intento dannoso

+0.5 - La violazione era dovuta a un’azione intenzionale, ad es. al fine di causare problemi al Titolare del trattamento (ad esempio, dimostrare la perdita di sicurezza) e/o al fine di danneggiare gli individui.

- Un dipendente di un'azienda condivide intenzionalmente i dati privati dei clienti in un sito pubblico sui social media.
- Un dipendente di un'azienda vende dati privati dai clienti a un'altra società.
- Un membro di un social network invia intenzionalmente informazioni sugli altri membri ai propri familiari al fine di danneggiarli.

Registro delle Violazioni dei dati

Il presente documento è istituito da

INSIT INDUSTRIA SPA

Identificativo nazionale (C.F.): 00937240042

al fine di documentare e dare evidenza degli adempimenti in caso di violazione dei dati personali (artt. 5, 24, 33, 34)

Luogo, Data Torino, 30/11/23

Firma

SIG.RA DEBENEDETTI ANNA

Dott.ssa Anna Debenedetti
DIRETTORE GENERALE
INSIT INDUSTRIA SPA

Pagina intenzionalmente vuota

Registro delle Violazioni dei Dati - RVD

#	Data annotazione	Data scoperta	Circostanze violazione	Natura della violazione	Conseguenze della violazione (ipotesi)	Misure e provvedimenti adottati	Valutazione dei rischi (appl. degli artt. 33 e 34 del GDPR)	Riferimenti notificazione (art. 33 del GDPR)	Riferimenti comunicazione (art. 34 del GDPR)	Riesame delle conseguenze (indicare la data del riesame)

Procedura per la gestione delle richieste degli interessati

Scopo

La presente procedura ha lo scopo di descrivere le attività che INSIT INDUSTRIA SPA deve porre in essere per gestire le richieste provenienti dagli interessati relativi ai diritti di quest'ultimi previsti dal Regolamento (UE) 2016/679.

Responsabilità

La responsabilità di tale attività ricade su:

- Delegato per la protezione dei dati
- Privacy Manager (PRI) o DPO, ove designato
- Eventuali responsabili del trattamento, se richiesto loro nelle istruzioni

Ambito di applicazione

Le persone fisiche (incluse ditte individuali e professionisti) i cui dati sono trattati INSIT INDUSTRIA SPA godono ai sensi del Regolamento (UE) 2016/679 dei seguenti diritti:

ACCESSO

cioè ottenere la conferma da parte di INSIT INDUSTRIA SPA che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

- le finalità del trattamento;
- le categorie di dati personali in questione;
- i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
- quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
- il diritto di proporre reclamo a un'autorità di controllo;
- qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;

- l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Quindi il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento.

RETTIFICA

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

CANCELLAZIONE

l'interessato ha il diritto di ottenere da INSIT INDUSTRIA SPA la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e INSIT INDUSTRIA SPA ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste **almeno uno dei motivi** seguenti:

- 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 ai sensi dell'articolo (finalità di marketing, inclusa profilazione, finalità di perseguire un legittimo interesse dell'Azienda ma non su base contrattuale o per obbligo di legge);
- 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.

OPPOSIZIONE AL TRATTAMENTO

L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano per la finalità di perseguire un legittimo interesse di INSIT INDUSTRIA SPA che non sia basato su un obbligo di legge o legato all'esecuzione di obblighi contrattuali. Può inoltre opporsi al trattamento per finalità di marketing e di profilazione.

I dati non devono essere cancellati (si veda sopra il diritto alla cancellazione) ma non possono più essere usati per le finalità indicate (legittimo interesse dell'Azienda, marketing, profilazione).

PORTABILITÀ

L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile (per es. file .CSV, .XML o MS Excel o altro formato in uso) da dispositivo automatico i dati personali che lo riguardano forniti a INSIT INDUSTRIA SPA e ha il diritto di trasmettere tali dati a un altro titolare del trattamento quando ricorrono **tutte le** seguenti **condizioni**:

- il trattamento si basi sul consenso o sia legato all'esecuzione di obblighi contrattuali; E
- il trattamento sia effettuato con mezzi automatizzati (no portabilità in caso di archivi cartacei).

L'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile (per es.: trasferimento dei dati direttamente da un operatore telefonico all'altro).

Verifica di efficacia della procedura

L'efficacia della presente procedura verrà valutata mediante audit annuale effettuato a volto a verificare la correttezza dello svolgimento della procedura.

Criteri applicabili

- Tenere in somma considerazione ogni richiesta degli interessati, agevolandoli
- Rispondere prontamente e tempestivamente (secondo le tempistiche previste), fornendo informazioni relative all'azione intrapresa riguardo ad ogni richiesta anche nel caso di impossibilità ad ottemperare.
- Tracciabilità e registrazione delle comunicazioni, comprensive delle informazioni temporali, sulla tipologia, sul mezzo di comunicazione e sulle valutazioni in merito alla richiesta (es. soddisfacibilità, difficoltà, infondatezza, ripetitività, costi, misure da adottare, misure adottate, ecc.) e le azioni intraprese, comprese le comunicazioni di risposta all'interessato. A tale scopo è istituito il **Registro delle Richieste e delle Comunicazioni con l'Interessato** (con acronimo **RRCI**).

Tutte le comunicazioni agli interessati sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici; le informazioni personali relative all'interessato possono essere fornite oralmente purché sia comprovata con altri mezzi (quindi non solo oralmente) l'identità dell'interessato.

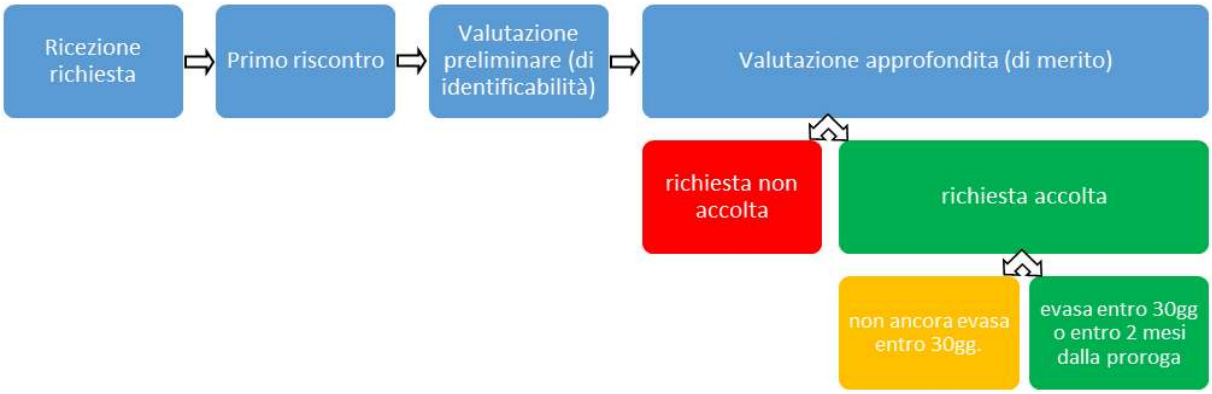
Qualora le finalità di un trattamento non prevedano l'identificazione dell'interessato, il soggetto giuridico comunica all'interessato che non c'è possibilità di identificarlo a meno che l'interessato, al fine di esercitare i propri diritti (artt.15-22 del GDPR), non fornisca ulteriori informazioni che ne consentano quindi l'identificazione.

Inoltre, qualora il soggetto giuridico nutra ragionevoli dubbi circa l'identità della persona fisica che presenta la richiesta di esercitare i propri diritti (artt.15-22 del GDPR), può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato.

In caso di richiesta di rettifica o cancellazione dei dati personali o limitazione del trattamento, qualora il soggetto giuridico accoglie favorevolmente tale richiesta, oltre a provvedervi direttamente e darne comunicazione all'interessato, provvede a comunicare a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate e/o da effettuare, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato, annotando comunque nel RRCI tra le misure intraprese ogni azione/decisione assunta.

Descrizione processo e definizione dei compiti

Ogni fase del processo è annotata nel **Registro delle Richieste e delle Comunicazioni con l'Interessato** (con acronimo **RRCI**).



Ricezione richiesta

Le eventuali richieste di accesso, rettifica, cancellazione, opposizione e portabilità saranno inviate dagli interessati, cosi come indicato nelle Informative predisposte da INSIT INDUSTRIA SPA, ad es. all'indirizzo e-mail dedicato.

Primo riscontro

L'interessato riceverà:

- immediatamente in via automatica, se configurato un risponditore,
- da parte del soggetto autorizzato a presidiare tale casella e-mail una comunicazione (preferibilmente e-mail) di conferma dell'avvenuta ricezione della richiesta con contenuto del tenore seguente:

> "*Gentile Signora, Egregio Signore,*
>
> *Le confermiamo la ricezione della e-mail in calce.*
>
> *Qualora la Sua e-mail riguardi la richiesta di esercitare uno dei diritti previsti dal Regolamento UE 679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (RGPD) e, in particolare, i diritti di accesso, rettifica, cancellazione, opposizione o portabilità dei Suoi dati personali, La informiamo che provvederemo a trattare la Sua richiesta il più rapidamente possibile e comunque entro 30 giorni dalla data odierna.*
>
> *Qualora, invece, la Sua richiesta non abbia ad oggetto l'esercizio di uno dei diritti di cui al paragrafo che precede, La invitiamo a contattarci ai ns. recapiti generici.*
>
> *Cordiali saluti*"

Valutazione preliminare

- Il RRI (e/o il DPO) determina se il soggetto che ha effettuato la richiesta sia identificato.
- In caso di mancata identificazione, il RRI (e/o il DPO) invia al richiedente una e-mail chiedendo di fornire i dati identificativi mancanti. Ad esempio:

> "*Gentile Signora, Egregio Signore,*
>
> *a fronte della sua richiesta di esercitare uno dei diritti previsti dal Regolamento UE 679/2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (RGPD), pervenutaci in data ... a mezzo email / …, non essendo stato possibile procedere alla sua identificazione, La invitiamo a ripresentare la Sua richiesta sul modello allegato, predisposto sulla base del modello pubblicato dall'Autorità italiana Garante per la protezione dei dati personali, semplificato in funzione della richiesta di cancellazione dei suoi dati ai sensi dell'art.17 del Reg.(UE)*

2016/679, così come pervenutaci. Nel caso non ricevessimo tale modello compilato unitamente a copia di un suo documento di identità in corso di validità, la Sua precedente richiesta sarà archiviata come non procedibile.

(*)

Distinti saluti"

(*) La risposta potrebbe già includere ulteriori elementi utili per sottolineare le cause ostative all'accoglimento delle richieste ad es. di cancellazione

"Inoltre, la informiamo che il diritto alla cancellazione non si applica nella misura in cui il trattamento sia necessario, tra l'altro, per l'adempimento di un obbligo giuridico o per motivi di interesse pubblico nel settore della sanità pubblica, come ad esempio nel caso della conservazione obbligatoria di documenti contabili, referti e altra documentazione sanitaria a cura di una struttura sanitaria, accreditata con il Servizio Sanitario Nazionale."

- Il RRI (e/o il DPO) determina la tipologia di richiesta (accesso, rettifica, cancellazione, opposizione e portabilità);

- Siccome le richieste possono pervenire nei formati e con i contenuti più disparati, nel caso in cui sia difficile circoscrivere le specifiche richieste dell'interessato, posto che si sia identificato adeguatamente, lo si può invitare a riformulare la propria richiesta utilizzando il modello predisposto dal Garante (cfr. https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/1089924), riportato in allegato. Tale modello è indirizzato al titolare del trattamento, anche per il tramite del Responsabile della Protezione dei Dati (RPD), ove designato dal titolare.

Valutazione approfondita

- Il RRI (e/o il DPO) valuta se sussistono i presupposti di legge per aderire alla richiesta dell'interessato.

- In caso di dubbi, il RRI (e/o il DPO) interpella il Delegato per la protezione dei dati o attiva un ulteriore consulto legale, chiedendo quale posizione adottare in merito alla richiesta dell'interessato. Alla luce di tale parere, il RRI (e/o il DPO) determina se aderire o meno alla richiesta dell'interessato

Se la richiesta non può essere accolta

Se il RRI (e/o il DPO) determina che non sussistono i presupposti per soddisfare la richiesta dell'interessato, invia allo stesso una comunicazione (preferibilmente e e-mail), informandolo del diniego e fornendo adeguata motivazione. Informa, altresì, l'interessato del diritto di proporre reclamo al Garante e di fare ricorso avanti il Giudice competente.

Quanto sopra deve essere fatto entro 30 giorni dalla richiesta.

Se la richiesta deve essere accolta

Se la richiesta dell'interessato deve essere accolta, il RRI (e/o il DPO) effettua, a seconda della tipologia di richiesta, le operazioni seguenti:

ACCESSO

- Il RRI (e/o il DPO), con il supporto delle competenti funzioni di Information and Communication Technology, ove necessario, determina quali dati dell'interessato siano detenuti da INSIT INDUSTRIA SPA e quali tipologie di trattamento dei dati sono effettuate.

● Il RRI (e/o il DPO) interpella eventuali Responsabili del trattamento dei dati (soggetti esterni che trattano dati per conto di INSIT INDUSTRIA SPA) per verificare se e quali trattamenti dei dati dell'interessato stiano effettuando.

● Il RRI (e/o il DPO) invia all'interessato la comunicazione con contenuto del tenore seguente:

"Gentile Signora / Egregio Signore,

facciamo seguito alla Sua gentile richiesta di avere accesso ai Suoi dati personali eventualmente trattati dalla nostra azienda per comunicarLe quanto segue:

☐ INSIT INDUSTRIA SPA NON risulta essere in possesso di dati personali che La riguardano.

☐ INSIT INDUSTRIA SPA è in possesso di dati personali a Lei riferibili, copia dei quali Le trasmettiamo nell'allegato alla presente e-mail.

(Se l'azienda è in possesso di dati personali a Lei riferibili) L'azienda tratta i Suoi dati personali per le seguenti finalità e per i periodi di seguito indicati:

☐ L'esecuzione di un contratto di cui Lei è parte o l'esecuzione di misure precontrattuali adottate su Sua richiesta. I Suoi dati sono trattati per il periodo necessario alla corretta e completa esecuzione del contratto.

☐ L'adempimento di un obbligo legale al quale la nostra azienda è soggetta (ad es.: per assolvere agli obblighi di natura fiscale e tributaria). I Suoi dati sono trattati per il periodo previsto dalla legge, in particolare dalle norme in materia di conservazione obbligatoria della documentazione fiscale e tributaria.

☐ La salvaguardia dei Suoi interessi vitali o di quelli di un'altra persona fisica. I Suoi dati sono trattati per il periodo strettamente necessario detti interessi vitali.

☐ L'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui la nostra azienda è stata investita. I Suoi dati sono trattati per il periodo necessario all'esecuzione del suddetto compito di interesse pubblico e per il periodo successivo eventualmente imposto dalle pubbliche amministrazioni affidatarie;

☐ La comunicazione di offerte commerciali, campagne di marketing, finalità per la quale Lei ha dato il Suo consenso. I Suoi dati sono trattati fintanto che l'azienda effettuerà tali attività oppure fintanto che Lei non revocherà il Suo consenso a tale tipologia di trattamento dei Suoi dati personali.

☐ Il perseguimento di un legittimo interesse della nostra azienda, e cioè per mantenere i contatti commerciali con Lei e continuare ad inviarLe offerte commerciali, informazioni sui prodotti, inviti ad eventi di natura commerciale e formativa.

I Suoi dati personali sono stati o potranno essere comunicati ai seguenti destinatari:

1. *nome azienda, indirizzo, contatti*
2. *….*
3. *….*

Come indicato nella informativa che Le trasmettiamo in allegato,

a) Lei ha diritto di chiedere al alla nostra azienda la rettifica/integrazione o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;

b) il diritto di proporre reclamo a un'autorità di controllo;

c) qualora i dati non siano raccolti presso l'interessato, di ottenere tutte le informazioni disponibili sulla loro origine;

d) essere informato sull'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato. In proposito la informiamo che la nostra azienda non effettua tali tipologie di trattamento.

Per qualsiasi ulteriore richiesta, La invitiamo a scriverci.

Cordiali saluti"

Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento può:

- addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta; oppure
- rifiutare di soddisfare la richiesta.

RETTIFICA O INTEGRAZIONE

- Il RRI (e/o il DPO) procede alla rettifica e/o all'integrazione dei dati personali secondo quanto richiesto dallo stesso.

- Il RRI (e/o il DPO) valuta e se del caso comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche effettuate e/o da effettuare

- Il RRI (e/o il DPO) invia all'interessato una comunicazione con contenuto del tenore seguente

"Gentile Signora / Egregio Signore,

facciamo seguito alla Sua gentile richiesta di rettifica e/o integrazione dei Suoi dati personali trattati dalla nostra azienda per comunicarLe che abbiamo provveduto alla rettifica e/o integrazione come da Lei richiesto.

I dati personali a Lei riferibili, trattati dalla nostra azienda, risultano, ad oggi, essere quelli indicati nell'allegato alla presente e-mail.

Per qualsiasi ulteriore richiesta, La invitiamo a scriverci.

Cordiali saluti"

CANCELLAZIONE

- Il RRI (e/o il DPO) procede alla cancellazione dei dati personali secondo quanto richiesto dallo stesso.

- Il RRI (e/o il DPO) valuta e se del caso comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali cancellazioni effettuate e/o da effettuare

- Il RRI (e/o il DPO) invia all'interessato una comunicazione con contenuto del tenore seguente

"Gentile Signora / Egregio Signore,

facciamo seguito alla Sua gentile richiesta di cancellazione dei Suoi dati personali trattati dalla nostra azienda per comunicarLe che:

☐ I Suoi dati personali sono trattati dalla nostra azienda esclusivamente per l'esecuzione di un contratto o per operazioni di natura precontrattuale da Lei richieste (ad es.: invio di un preventivo, catalogo, offerta, ecc. da Lei richiesto), ovvero in adempimento di un obbligo di legge. Pertanto, la cancellazione dei Suoi dati non è possibile fintanto che i nostri obblighi di natura contrattuale, precontrattuale o di natura legale non saranno terminati.

☐ Abbiamo provveduto a cancellare i Suoi dati personali che non verranno, pertanto, più trattati dalla nostra azienda. A seguito della presente comunicazione, provvederemo a cancellare anche il Suo indirizzo e-mail dai nostri database. La informiamo, tuttavia, che qualora i Suoi dati fossero trattati per finalità connesse all'esecuzione di un contratto (ad es.: spedizione di prodotti da Lei acquistati), per l'esecuzione di obblighi di natura precontrattuale (ad es.: invio di un preventivo, catalogo, offerta, ecc. da Lei richiesto) o in adempimento di obblighi di legge (ad es.: conservazione fatture, bollette doganali, ecc.), i Suoi dati saranno conservati dalla nostra azienda però al fine esclusivo di adempiere a tali obblighi.

Per qualsiasi ulteriore richiesta, La invitiamo a scriverci.

Cordiali saluti"

OPPOSIZIONE O LIMITAZIONE DEL TRATTAMENTO

● Il RRI (e/o il DPO) determina quali dati dell'interessato sono trattati per la finalità di perseguire un legittimo interesse dell'Azienda che non sia basato su un obbligo di legge o legato all'esecuzione di obblighi contrattuali o per finalità di marketing inclusa la profilazione.

● Il RRI (e/o il DPO), col supporto del Responsabile ICT mette in atto le misure necessarie affinché tali dati non siano più utilizzati per le finalità ora indicate (ma siano trattabili per altre finalità legittime).

● Il RRI (e/o il DPO) valuta e se del caso comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali limitazioni del trattamento effettuate e/o da effettuare

● Il RRI (e/o il DPO) invia all'interessato una comunicazione con contenuto del tenore seguente

"Gentile Signora / Egregio Signore,

facciamo seguito alla Sua gentile richiesta di opposizione al trattamento dei Suoi dati personali per finalità basate su un legittimo interesse della nostra azienda ad effettuare tale trattamento, così come definito all'articolo 6, paragrafo 1, lettera f) del Regolamento UE 679/2016 (GDPR), per comunicarLe che:

A partire dalla data odierna, i Suoi dati personali non saranno più trattati dalla nostra azienda per il perseguimento della finalità di cui sopra e, conseguentemente, non riceverà più, ad esempio, comunicazioni di marketing diretto da parte della nostra azienda.

Per qualsiasi ulteriore richiesta, La invitiamo a scriverci.

Cordiali saluti"

PORTABILITA'

● Il RRI (e/o il DPO) predisponendo file (per es. file .CSV, .XML o MS Excel o altro formato in uso comune nel settore) contenente i dati personali dell'interessato.

- Il RRI (e/o il DPO) trasmette tale file all'interessato con contenuto del tenore seguente

> *"Gentile Signora / Egregio Signore,*
>
> *facciamo seguito alla Sua gentile richiesta di portabilità dei Suoi dati personali trattati dalla nostra azienda per trasmetterLe, in allegato, il file contenente i dati personali a Lei riferibili attualmente in possesso della nostra azienda.*
>
> *Il file è stato predisposto in formato …… ritenendo che tale file sia di uso comune e di facile accessibilità per Lei.*
>
> *Per qualsiasi ulteriore richiesta, La invitiamo a scriverci.*
>
> *Cordiali saluti"*

Se la richiesta non è evasa entro 30 giorni

Il termine, nel caso di esercizio dei diritti di cui agli articoli da 15 a 22 del GDPR, può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Il RRI (e/o il DPO) informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta.

> *"Gentile Signora / Egregio Signore,*
>
> *facciamo seguito alla Sua gentile richiesta di esercitare uno dei diritti previsti dal Regolamento UE 679/2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (GDPR), pervenutaci in data ... a mezzo email / …, per informarla che, non essendo ancora stato possibile darvi compiutamente seguito* tenuto conto della complessità della Sua richiesta e del delle ulteriori richieste da Lei formulate nonché del numero complessivo delle ulteriori richieste ricevute da terzi, il termine per fornirle una risposta è prorogato di ulteriori due mesi rispetto alla prima scadenza (un mese dalla ricezione della sua richiesta) ai sensi dell'art.12 co.3 del GDPR.
>
> Pertanto, entro il nuovo termine del … provvederemo a darle riscontro.
>
> *Cordiali saluti"*

Se la richiesta è evasa entro 30 giorni o entro 2 mesi dalla proroga

La procedura è stata completata correttamente. Il RRI (e/o il DPO) conserva le trascrizioni su RRCI e la documentazione atta a dimostrare di aver trattato correttamente la richiesta dell'interessato.

All'attenzione di

INSIT INDUSTRIA SPA

ESERCIZIO DI DIRITTI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

(artt. 15-22 del Regolamento (UE) 2016/679)

Il/La sottoscritto/a…….

nato/a a……. il……, esercita con la presente richiesta i seguenti diritti di cui agli artt. 15-22 del Regolamento (UE) 2016/679:

1. Accesso ai dati personali

(art. 15 del Regolamento (UE) 2016/679)

Il sottoscritto *(barrare solo le caselle che interessano)*:

☐ chiede conferma che sia o meno in corso un trattamento di dati personali che lo riguardano;
☐ in caso di conferma, chiede di ottenere l'accesso a tali dati, una copia degli stessi, e tutte le informazioni previste alle lettere da a) a h) dell'art. 15, paragrafo 1, del Regolamento (UE) 2016/679, e in particolare;

- le finalità del trattamento;
- le categorie di dati personali trattate;
- i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
- il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'origine dei dati (ovvero il soggetto o la specifica fonte dalla quale essi sono stati acquisiti);
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e le informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

2. Richiesta di intervento sui dati

(artt. 16-18 del Regolamento (UE) 2016/679)

Il sottoscritto chiede di effettuare le seguenti operazioni *(barrare solo le caselle che interessano)*:

- ☐ rettificazione e/o aggiornamento dei dati (art. 16 del Regolamento (UE) 2016/679);
- ☐ cancellazione dei dati (art. 17, paragrafo 1, del Regolamento (UE) 2016/679), per i seguenti motivi *(specificare quali)*:

  a)…;

  b)….;

  c)…;

  nei casi previsti all'art. 17, paragrafo 2, del Regolamento (UE) 2016/679, l'attestazione che il titolare ha informato altri titolari di trattamento della richiesta dell'interessato di cancellare link, copie o riproduzioni dei suoi dati personali;
- ☐ limitazione del trattamento (art. 18) per i seguenti motivi *(barrare le caselle che interessano)*:
  - ☐ contesta l'esattezza dei dati personali;
  - ☐ il trattamento dei dati è illecito;
  - ☐ i dati sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
  - ☐ l'interessato si è opposto al trattamento dei dati ai sensi dell'art. 21, paragrafo 1, del Regolamento (UE) 2016/679.

La presente richiesta riguarda (indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento):

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

3.Portabilità dei dati[3]

(art. 20 del Regolamento (UE) 2016/679)

Con riferimento a tutti i dati personali forniti al titolare, il sottoscritto chiede di *(barrare solo le caselle che interessano)*:

- ☐ ricevere tali dati in un formato strutturato, di uso comune e leggibile da dispositivo automatico;
- ☐ trasmettere direttamente al seguente diverso titolare del trattamento *(specificare i riferimenti identificativi e di contatto del titolare: ……):*
  - ☐ tutti i dati personali forniti al titolare;
  - ☐ un sottoinsieme di tali dati.

[3] Per approfondimenti: Linee-guida sul diritto alla "portabilità dei dati" - WP242, adottate dal Gruppo di lavoro Art. 29, disponibili in www.garanteprivacy.it/regolamentoue/portabilita.

La presente richiesta riguarda (indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento):

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

4. Opposizione al trattamento

(art. 21, paragrafo 1 del Regolamento (UE) 2016/679)

☐ Il sottoscritto si oppone al trattamento dei suoi dati personali ai sensi dell'art. 6, paragrafo 1, lettera e) o lettera f), per i seguenti motivi legati alla sua situazione particolare (specificare):

_____
_____
_____
_____
_____
_____
_____

5. Opposizione al trattamento per fini di marketing diretto

(art. 21, paragrafo 2 del Regolamento (UE) 2016/679)

☐ Il sottoscritto si oppone al trattamento dei dati effettuato a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Il sottoscritto:

☐ Chiede di essere informato, ai sensi dell'art. 12, paragrafo 4 del Regolamento (UE) 2016/679, al più tardi entro un mese dal ricevimento della presente richiesta, degli eventuali motivi che impediscono al titolare di fornire le informazioni o svolgere le operazioni richieste.

☐ Chiede, in particolare, di essere informato della sussistenza di eventuali condizioni che impediscono al titolare di identificarlo come interessato, ai sensi dell'art. 11, paragrafo 2, del Regolamento (UE) 2016/679.

Recapito per la risposta[4]**:**

Via/Piazza

Comune Provincia Codice postale

oppure

e-mail/PEC:

Eventuali precisazioni

Il sottoscritto precisa (fornire eventuali spiegazioni utili o indicare eventuali documenti allegati):

_____
_____
_____
_____
_____
_____
_____

(Luogo e data)

(Firma)

[4] Allegare copia di un documento di riconoscimento

All'attenzione di

INSIT INDUSTRIA SPA

MODELLO DI REVOCA DEL CONSENSO DEGLI INTERESSATI

(artt. 7 del Regolamento (UE) 2016/679)

Il/La sottoscritto/a…….

nato/a a……. il……., esercita con la presente la REVOCA del consenso al trattamento dei miei dati da parte di INSIT INDUSTRIA SPA precedentemente fornito ai fini di:

marketing diretto via e-mail o altri mezzi
della propria immagine/audio/video (e/o eventuale trascrizione testuale/descrittiva) fuori dai casi diversamente regolati da contratti.
pagamento con carta di credito / assegno / carta di debito
altro (specificare)
_____
_____
_____
_____

Questa revoca non pregiudica la liceità delle attività di trattamento svolte fino ad allora, vale a dire la possibilità di fornire un nuovo consenso in futuro.

Il sottoscritto:

- ☐ Chiede di essere informato, ai sensi dell'art. 12, paragrafo 4 del Regolamento (UE) 2016/679, al più tardi entro un mese dal ricevimento della presente richiesta, degli eventuali motivi che impediscono al titolare di fornire le informazioni o svolgere le operazioni richieste.
- ☐ Chiede, in particolare, di essere informato della sussistenza di eventuali condizioni che impediscono al titolare di identificarlo come interessato, ai sensi dell'art. 11, paragrafo 2, del Regolamento (UE) 2016/679.

Recapito per la risposta[5]**:**

Via/Piazza

Comune Provincia Codice postale

[5] Allegare copia di un documento di riconoscimento

oppure

e-mail/PEC:

Eventuali precisazioni

Il sottoscritto precisa (fornire eventuali spiegazioni utili o indicare eventuali documenti allegati):

_____
_____
_____
_____
_____
_____
_____

(Luogo e data)

(Firma)

Registro delle Richieste e delle Comunicazioni con l'Interessato

Il presente documento è istituito da

INSIT INDUSTRIA SPA

Identificativo nazionale (C.F.): 00937240042

al fine di documentare e dare evidenza del processo di comunicazione e di risposta all'esercizio dei diritti dell'interessato (artt. 11, 12, 15-22,34)

Luogo, Data Torino, 30/11/23

Firma

SIG.RA DEBENEDETTI ANNA

Dott.ssa Anna Debenedetti
DIRETTORE GENERALE
INSIT INDUSTRIA SPA

Pagina intenzionalmente vuota

Parte 1 – Richieste (ingresso)

#	data	Oggetto della richiesta	Rif. norma	Interessato	Mezzo	Rintracciabilità della richiesta	Valutazioni	Azioni intraprese	Rif.Comunicazioni all'interessato	Rif.Comunicazioni a terzi

Parte 2 – Comunicazioni (uscita)

#	data	Rif.Richiesta	Rif. norma	Tipo (interessato / terzi)	Mezzo	Destinatario	Oggetto della comunicazione	Rintracciabilità della comunicazione

ISTRUZIONI PER LA COMPILAZIONE DEL RRCI		
Parte 1 – Richieste (ingresso)		
Campo	**Istruzione**	**Esempio**
#R	Inserire numero progressivo (o un codice) identificativo della richiesta ricevuta	*1, 2,……..100…* *R.01, R.02, ……..R.100…*
Data	Inserire la data di ricezione della richiesta	*gg/mm/aaaa*
Oggetto della richiesta	Indicare l'oggetto della richiesta pervenuta	*Richiesta informazioni su quali dati personali sono trattati nell'ambito del trattamento…* *Richiesta cancellazione dei dati personali forniti tramite portale..*
Rif. norma	Indicare il riferimento normativo a cui fa capo la richiesta dell'interessato	*Art. 15 del GDPR Diritto di accesso dell'Interessato*
Interessato	Indicare nome e cognome dell'Interessato	
Mezzo	Indicare il mezzo di comunicazione con il quale è pervenuta la richiesta	*E-mail* *PEC* *Contatto telefonico* *Richiesta diretta di persona* *Lettera postale*
Rintracciabilità della richiesta	Indicare tutti i riferimenti utili al fine di identificare e rintracciare agevolmente la richiesta	*E-mail ricevuta in data xxx all'indirizzo yyy con oggetto: "zzz" ed archiviata nella cartella al percorso ……..* *Prot. In ingresso XYZ*
Valutazioni	Indicare se il soggetto che ha effettuato la richiesta sia stato identificato Indicare la categoria di interessato di appartenenza Indicare se sussistono i presupposti di legge per aderire alla richiesta dell'interessato e motivare la valutazione soddisfacibilità, difficoltà, infondatezza, ripetitività, costi della richiesta	*Il soggetto è stato identificato in quanto lavoratore dipendete/utente del portale…* *lavoratore dipendete, familiare del lavoratore, collaboratore, fornitore, cliente, utenti web, docenti, allievi, terzi, ecc* *Il soggetto è stato identificato a seguito di approfondimento dell'identità* *A seguito di valutazione dei presupposti di legge, la richiesta (non) può essere accolta in quanto….(motivare la valutazione)*
Azioni intraprese	Indicare quali azioni sono state intraprese al fine di dar seguito alla richiesta dell'interessato	*invio primo riscontro di conferma dell'avvenuta ricezione della richiesta* *verifica della sussistenza legittima della richiesta* *richiesta di ulteriori dettagli all'interessato* *Invio riscontro finale con esito della richiesta*

Rif. Comunicazioni all'interessato	Riportare il numero progressivo (o il codice) identificativo della comunicazione indicato al campo **#C** nella Parte 2 – Comunicazioni (uscita)	*1, 2,……..100…* *C.01, C.02, ……..C.100…*
Rif. Comunicazioni a terzi	Riportare il numero progressivo (o il codice) identificativo della comunicazione indicato al campo **#C** nella Parte 2 – Comunicazioni (uscita)	*1, 2,……..100…* *C.01, C.02, ……..C.100…*
Parte 2 – Comunicazioni (uscita)		
Campo	**Istruzione**	***Esempio***
#C	Inserire numero progressivo (o codice) identificativo della comunicazione inviata all'Interessato	*1, 2,……..100…* *C.01, C.02, ……..C.100…*
Data	Inserire la data di ricezione della richiesta	*gg/mm/aaaa*
Rif. Richiesta	Riportare il numero progressivo (o il codice) identificativo della richiesta indicato al campo **#R** nella Parte 1 – Richieste (ingresso)	*1, 2,……..100…* *R.01, R.02, ……..R.100…*
Rif. norma	Indicare il riferimento normativo a cui fa capo la comunicazione in risposta all'interessato	*Art. 15 del GDPR Diritto di accesso dell'Interessato*
Tipo (interessato / terzi)	Indicare se la comunicazione è inoltrata all'Interessato o a Terzi	*Interessato* *Terzi*
Mezzo	Indicare il mezzo con il quale è inviata la comunicazione	*E-mail ordinaria* *PEC* *Contatto telefonico* *Richiesta diretta di persona* *Lettera postale*
Destinatario	Indicare i riferimenti del destinatario	*nome e cognome* *indirizzo mail* *ragione sociale*
Oggetto della comunicazione	Indicare l'oggetto della comunicazione	*invio primo riscontro di conferma dell'avvenuta ricezione della richiesta* *richiesta ulteriori dettagli all'interessato* *Invio riscontro finale con esito della richiesta* *richiesta di dettaglio sui termini di cancellazione al Fornitore XY*
Rintracciabilità della comunicazione	Indicare tutti i riferimenti utili al fine di identificare e rintracciare agevolmente la comunicazione	*E-mail inviata in data xxx all'indirizzo yyy con oggetto: "zzz" ed archiviata nella cartella al percorso ……..* *Prot. In uscita XYZ*

Procedura per la distruzione e smaltimento di documenti cartacei contenenti dati personali

Scopo

La presente procedura ha lo scopo di descrivere le attività che si devono svolgere per gestire la distruzione e smaltimento di documenti cartacei contenenti, tra l'altro, dati personali tutelati ai sensi del Regolamento (UE) 2016/679.

Responsabilità

La responsabilità è così suddivisa:

Applicazione della procedura	Tutto il personale
Revisione della procedura	Preposto alla sicurezza del trattamento dei dati
Approvazione della procedura	Delegato per la protezione dei dati

Ambito di applicazione

La procedura si applica solo ai supporti cartacei documentali.

- quando un singolo documento non deve essere archiviato, ad es. per errore o perché non più utile, deve essere distrutto secondo procedura;
- quando un archivio o raccolta di documenti (dossier, faldoni, ecc.) non deve più essere conservato, ad es. perché si è raggiunto il limite temporale di conservazione massima, deve essere smaltito secondo procedura.

La procedura non si applica

- per l'archiviazione corrente
- per l'archiviazione a lunga-conservazione
- per supporti informatici

Per le operazioni di distruzione o smaltimento occorre conoscere la classificazione dei documenti e/o la tipologia del contenuto (ad es. dati riservati, confidenziali, segreti, personali, sensibili, giudiziari, particolari, sanitari, biometrici, genetici, ecc.).

In caso di una raccolta di documenti non gestita, occorre prima rivederli per determinare se alcuni sono ridondanti e possono essere distrutti e per gestire il resto per il trasferimento in un archivio gestito.

Distruzione dei documenti

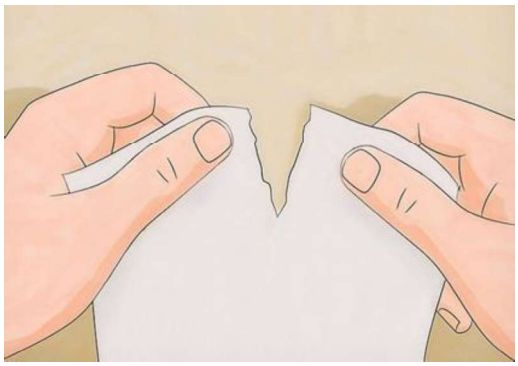
Un documento si considera distrutto quando il supporto cartaceo originale viene strappato o tagliato in una o più parti; dopo tale distruzione, le parti risultanti del supporto cartaceo (ritagli, strisce, pezzi, ecc.) sono da considerarsi rifiuti e devono essere gettate nell'immondizia, eventualmente secondo le regole di separazione del materiale a fini del riciclo.

La distruzione del documento, a seconda della sua classificazione e/o della tipologia del contenuto in esso presente, può avvenire nelle seguenti diverse modalità:

Tipo documento / contenuto	Strappo	Triturazione
Documento pubblico	Sì, in almeno 2 parti (*)	Sì
Documento ad uso interno	Sì, in almeno 2 parti	Sì
Documento riservato	Sì, in almeno 4 parti	Sì, consigliato
Documento confidenziale	Sì, in almeno 8 parti	Sì, consigliato
Documento strettamente confidenziale	Sì, in almeno 8 parti	Sì, consigliato
Documento segreto	Non ammesso	Sì, obbligatorio
Contenuto con dati non personali e non riservati	Sì, in almeno 2 parti (*)	Sì
Contenuto con dati non personali ma riservati	Sì, in almeno 4 parti	Sì, consigliato
Contenuto con dati personali comuni (nome, cognome, indirizzo, email, telefono, ecc.)	Sì, in almeno 2 parti	Sì
Contenuto con dati personali economici riservati (es. coordinate bancarie, numeri di conti corrente, numeri di carte di credito, codici fiscali, ecc.)	Sì, in almeno 4 parti	Sì, consigliato
Contenuto con dati sensibili (es. cedolini paghe, permessi di soggiorno, denunce di infortuni e malattie professionali, invalidità)	Sì, in almeno 8 parti	Sì, consigliato
Contenuto con dati personali appartenenti a categorie particolari	Sì, in almeno 8 parti	Sì, consigliato
Contenuto con dati sanitari e sullo stato di salute (certificati medici, referti, analisi cliniche, radiografie, ecc.)	Sì, in almeno 8 parti	Sì, consigliato
Contenuto con dati su orientamento politico, adesione a sindacati o partiti	Sì, in almeno 8 parti	Sì, consigliato
Contenuto con dati su orientamento religioso/filosofico, adesione a movimenti/confessioni religiose/filosofiche	Sì, in almeno 8 parti	Sì, consigliato
Contenuto con dati biometrici (es. impronte digitali)	Sì, in almeno 8 parti	Sì, consigliato
Contenuto con dati genetici	Sì, in almeno 8 parti	Sì, consigliato
Contenuto con dati sull'orientamento e la vita sessuale	Sì, in almeno 8 parti	Sì, consigliato
Contenuto con dati giudiziari (es. fedina penale, casellario giudiziale, sanzioni, provvedimenti interdittivi, ecc.)	Sì, in almeno 8 parti	Sì, consigliato

In deroga, è possibile gettare tra i rifiuti un documento senza prima distruggerlo solo se il documento è classificato come “pubblico” o se non contiene dati personali o non contiene dati riservati.

Strappo



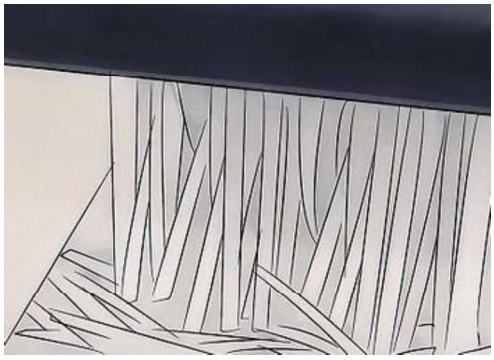
● Per strappare un foglio, occorre romperlo in due o più pezzi, lacerandolo o stracciandolo.

● Questo metodo può essere adottato solo se si ha una quantità relativamente modesta di carta da distruggere, poiché ciò può richiedere molto tempo e, come movimento ripetitivo, può generare disturbi e affaticamento.

● Questo metodo non è consigliato per smaltire documenti che contengono informazioni riservate e dati sensibili. Se si adotta questo metodo, assicurarsi di strappare la carta in pezzi molto piccoli: più sono piccoli, maggiore sarà la sicurezza che il contenuto non si possa più ricostruire.

Triturazione

Per la triturazione occorre un distruggidocumenti, di cui occorre seguire attentamente il manuale di istruzioni:



● controllare il numero massimo di fogli inseribili: infatti, il distruggidocumenti potrebbe incepparsi molto facilmente se si tenta di passare troppi fogli contemporaneamente.

● controllare quali articoli non devono essere triturati: alcuni distruggidocumenti possono facilmente distruggere finestre di plastica, graffette e persino carte di credito

● se si supera la capacità o si distrugge l'articolo sbagliato e si finisce con un inceppamento della carta, il distruggidocumenti dovrebbe essere dotato di una modalità inversa che consente di rimuovere facilmente l'inceppamento.

● dopo aver terminato con la triturazione, spegnere il distruggidocumenti: infatti, lasciarlo acceso per troppo tempo può surriscaldarne il motore.

● oliare regolarmente il distruggidocumenti per mantenerlo funzionante in modo ottimale.

Per scegliere ed approvvigionare un distruggidocumenti, seguire le seguenti indicazioni

● con un efficace meccanismo di taglio per evitare inceppamenti della carta;

● con una geometria e capacità di carico adeguata al volume e forma dei documenti da distruggere;

● con una affidabilità del sistema di taglio adeguata alla frequenza ed intensità d’uso;

● con uno spazio tra le lame che tagliano le strisce adeguato al tipo di documento da distruggere: ad es. nel caso di dati riservati, considerare una larghezza massima delle strisce di 5 cm;

con protezioni e/o blocchi di sicurezza e protezione per evitare infortuni.

Smaltimento degli archivi

Smaltire gli archivi significa disfarsene in modo appropriato evitando per quanto possibile che i dati presenti nei documenti cartacei di cui ci si libera possano essere acquisiti da terzi malintenzionati ed in particolare che non si verifichino possibilità di furto di identità delle persone.

Tutte gli smaltimenti devono essere documentati con un report di smaltimento che riporti data, descrizione dell'archivio smaltito, soggetto che ha eseguito lo smaltimento e descrizione della modalità seguita.

Si possono smaltire in autonomia archivi di modeste dimensioni e volumi, distruggendoli internamente secondo la procedura per la distruzione dei documenti, estraendo dall'archivio un documento alla volta o piccoli fascicoli; lo smaltimento di volumi maggiori deve essere organizzato pianificato, rivolgendosi preferibilmente ad aziende specializzate nello smaltimento e macero di documenti che possano eventualmente procedere sul posto e che rilascino un certificato di distruzione.