LINEA GUIDA

Linea Guida per la tutela dei dati fin dalla progettazione attraverso modalità di protezione a impostazione predefinita (Privacy by Design - Privacy by Default)

Rev.	Data	Oggetto	Responsabilità
/	29/06/2022	Aggiornamento del documento	**Elaborato da**: Avvera S.r.l.
			Verificato da: Cin S.p.A
			Approvato da: Cin S.p.A

INDICE

1. PREMESSA

Il Regolamento UE 2016/679 (GDPR) richiede che la tutela dei diritti e delle libertà degli interessati con riguardo al trattamento dei dati personali comporti l'attuazione di adeguate misure tecniche e organizzative a tutela dei dati personali fin dalla progettazione (**privacy by design**) e così per tutto il ciclo vita dei dati stessi come impostazione predefinita (**privacy by default**).

La società ha, quindi, predisposto un sistema di tutela dei dati personali volto a garantire la protezione degli stessi sin dalle prime fasi di trattamento fino a tutto il loro ciclo vita con l'adozione di specifici meccanismi volti a presidiare i dati personali nella loro:

1. **riservatezza**, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale.
2. **integrità**, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale.
3. **disponibilità**, ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.
4. **resilienza**, ovvero la capacità di un sistema di adattarsi ai cambiamenti.

La società si pone l'obiettivo di osservare il principio della privacy by default rispettando i principi generali della protezione dei dati, quali la minimizzazione dei dati e la limitazione delle finalità, garantendo, quindi, che:

1. i dati personali trattati siano solo quelli necessari per la finalità specifica del trattamento;
2. i dati personali siano resi accessibili sono a determinate persone con esclusione, quindi, di terzi non autorizzati;
3. i dati raccolti non siano conservati per tempi ulteriori rispetto a quelli minimi necessari.

La presente linea guida delinea le responsabilità e le modalità di tutela del dato fin dalla progettazione del trattamento attraverso modalità di protezione a impostazione predefinita per assicurarne una corretta conduzione.

2. AMBITO DI APPLICAZIONE

I principi disciplinati dal presente documento si applicano al momento di determinare i mezzi del trattamento di dati personali nonché all'atto del trattamento stesso. La società tiene conto del diritto alla protezione dei dati:

1. dalle prime fasi del processo di sviluppo e progettazione dei prodotti, servizi ed applicazioni;
2. in ogni variazione del prodotto e servizio offerto, della struttura organizzativa, informatica o logistica a supporto, dei processi aziendali;
3. al momento della partecipazione a bandi di gara.

3. RESPONSABILITÀ DI ATTUAZIONE

Responsabile dell'attuazione della presente linea guida, di concerto con il Titolare del Trattamento, è il Responsabile IT ed il Responsabile di area competente.

4. DISTRIBUZIONE

La presente procedura ha come destinatari tutto il personale di CIN S.p.A.

5. DEFINIZIONI

Termine	Definizione
Coordinatore privacy	La persona fisica che, all'interno della struttura gerarchica del Titolare del trattamento, è preposta da quest'ultimo a concorrere alla determinazione delle modalità e finalità del trattamento
Danneggiamento	Evento che colpisce il dato personale e ha come conseguenza che il dato stesso è stato modificato, danneggiato o comunque non è più integro.
Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Disponibilità	Caratteristica del dato personale che indica l'accessibilità dello stesso a chi ne ha diritto e nel momento in cui servono.
Distruzione	Evento che colpisce il dato personale e ha come conseguenza che il dato stesso non esiste più o non esiste in una forma utilizzabile dal titolare del trattamento.
DPO/RPD	Data Protection Officer / Responsabile della Protezione dei Dati.
GDPR/RGPD	General Data Protection Regulation (Regolamento UE 2016/679) / Regolamento generale sulla protezione dei dati (Regolamento UE 2016/679)
Integrità	Caratteristica del dato personale che ricomprende elementi di correttezza, coerenza, affidabilità e completezza.
Interessato	La persona fisica a cui si riferiscono i dati personali.
Perdita	Evento che colpisce il dato personale e ha come conseguenza che il titolare ne ha perso il controllo, l'accesso o la proprietà.
Persona autorizzata al trattamento	Chiunque agisca sotto l'autorità del titolare o del Coordinatore Provacy, che abbia accesso a dati personali e che sia istruito in tal senso.
Responsabile del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.
Riservatezza	Caratteristica del dato personale che non deve essere disponibile o divulgata a terzi.
Terzo	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.
Titolare del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

Termine	Definizione
Trattamento non autorizzato o non conforme alla legge	Evento che colpisce il dato personale e ha come conseguenza che esso diviene visibile a terzi o che terzi vi effettuano trattamenti in assenza di un titolo autorizzativo.
Violazione dei dati personali	La violazione di sicurezza (breach of security) che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati
Violazione della disponibilità	La violazione della disponibilità consiste in una perdita di accesso o distruzione di dati personali non autorizzata o casuale.
Violazione della integrità	La violazione della integrità consiste in una modifica di dati personali non autorizzata o casuale.
Violazione della riservatezza	La violazione della riservatezza consiste in una visibilità o un accesso a dati personali non autorizzata o casuale.

6. PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PER IMPOSTAZIONE PREDEFINITA

Al momento dello sviluppo, progettazione, selezione ed utilizzo di un software o di un servizio e prodotto, in ogni variazione del prodotto e servizio offerto, della struttura organizzativa, informatica o logistica a supporto, nei processi aziendali ovvero al momento della partecipazione a bandi di gara:

1. il Responsabile di Area competente con la collaborazione del Responsabile IT deve:
   - individuare i soli dati personali che sono interessati dall'applicativo;
   - procedere ad una valutazione del rischio sulla riservatezza, integrità, disponibilità di tali dati;
   - analizzare lo stato dell'arte tecnologico, i costi di attuazione, la natura, l'ambito di applicazione, il contesto e le finalità del trattamento, la valutazione del rischio effettuata in ordine alle possibili misure tecniche ed organizzative da adottare a protezione dei dati personali;
   - relazionare – se del caso - il Titolare del trattamento o il DPO sull'esito dell'analisi.

2. il Responsabile di Area competente con la collaborazione del Responsabile IT, di concerto con il Responsabile della Protezione dei Dati, deve definire e relazionare il titolare circa le misure tecniche ed organizzative da adottare per garantire la necessaria protezione dei dati personali trattati:
   - riducendo al minimo il trattamento dei dati personali,
   - circoscrivendo gli standard architetturali necessari a soddisfare i requisiti di sicurezza definiti,
   - definendo delle tecniche di Data masking quali la pseudonomizzazione, sia se utilizzati in ambienti di test e/o di training sia se ne è previsto l'utilizzo in ambienti diversi da quello di produzione,
   - agevolando l'interessato al controllo sul trattamento dei propri dati,
   - prevedendo delle attività di Vulnerability management per verificare l'efficacia e l'efficienza delle misure di sicurezza e degli standard applicativi e strutturali implementati (penetration test, vulnerability assessment, etc.),
   - predisponendo periodiche attività di formazione, per istruire i tecnici sugli standard di programmazione sicura e sulle architetture sicure e favorendo la "awareness" al fine di sensibilizzare il personale sugli aspetti e le implicazioni inerenti la protezione e la gestione dei dati personali.

Il Titolare del trattamento o un suo delegato sulla base delle informazioni fornite e consulenze ricevute, deve definire le misure di sicurezza tecniche ed organizzative adeguate ad assicurare la protezione dei dati personali oggetto di trattamento.

Il Responsabile di Area competente con la collaborazione del Responsabile IT predispone con cadenza periodica un piano di audit al fine di verificare che:

- le misure tecniche ed organizzative adottate siano adeguate a garantire e dimostrare che il trattamento è conforme alle disposizioni normative;
- tali misure siano oggetto di periodico riesame ed aggiornamento;
- tali misure siano efficaci in relazione alla natura, all'ambito di applicazione e alle finalità del trattamento;
- siano trattati solo i dati necessari per ogni specifica finalità di trattamento.

7. PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PER IMPOSTAZIONE PREDEFINITA IN FASE DI PRE-QUALIFICAZIONE DEL FORNITORE

Per la partecipazione del fornitore ai processi negoziali, La società prevede la valutazione dei requisiti di protezione e sicurezza sui dati personali oggetto di trattamento.

In sede di pre-qualificazione e in costanza di rapporto, il fornitore dovrà dare garanzia di adottare tutte le misure di sicurezza implementate da La società a protezione dei dati personali e per il trattamento dei quali è richiesto il suo servizio, potendo, se del caso, aumentarle discrezionalmente ma in nessun caso ridurle.

Occorre, inoltre, prevedere clausole contrattuali che consentano, oltre alle garanzie di cui sopra, la possibilità di effettuare audit di seconda parte sul fornitore sia in sede di pre-qualificazione sia durante il mantenimento del rapporto contrattuale.