Howden Assiteca Consulting

Registro del trattamento ai fini della normativa sul trattamento dei dati

Trattamento dei dati personali
Regolamento Europeo sulla Tutela dei dati personali (UE 2016/679) e normativa vigente

HOWDEN

Agenda

1. Accenni di normativa
2. Cosa devono fare le organizzazioni
3. Istruzioni per la compilazione del registro
4. Case Study

Cos’è la protezione dei dati personali

La tutela della Privacy

È il diritto di ciascuno individuo di conoscere, controllare ed eventualmente rifiutare il trattamento dei propri dati personali effettuato da soggetti terzi.

Ad oggi, in Italia, sono applicabili **più normative** che disciplinano la privacy:

- D. Lgs. **196/2003**: “Codice in materia di privacy”;
- D. Lgs. **101/2018**, che ha modificato il Codice Privacy;
- **Regolamento** Europeo in materia di protezione dei dati personali **EU 679/2016** (cosiddetto GDPR).

Dati Personali (Art. 4)

Tutte le informazioni relative ad un individuo

Dato personale è 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.

Categorie particolari di dati personali (ex dati sensibili):

- origine razziale ed etnica
- convinzioni religiose, filosofiche o di altro genere
- opinioni politiche
- adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale
- stato di salute e la vita sessuale

Tutte le operazioni fisiche o informatiche

Dati Personali (Art. 4)

Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come:

- la **raccolta**, la **registrazione**, **l'organizzazione**, la **strutturazione**;
- la **conservazione**, **l'adattamento** o la **modifica**;
- **l'estrazione**, la **consultazione**, **l'uso**;
- la **comunicazione** mediante trasmissione, **diffusione** o qualsiasi altra forma di messa a disposizione, il **raffronto** o l'interconnessione;
- la **limitazione**, la **cancellazione** o la **distruzione**.

Le regole generali
Principi del trattamento (Art. 5)

Principi generali applicabili al trattamento:

- **liceità**, **correttezza** e **trasparenza** nei confronti dell'interessato;
- **limitazione** delle finalità;
- **minimizzazione** dei dati;
- **esattezza**;
- **limitazione** della **conservazione**;
- **integrità** e **riservatezza**.

Diritti dell'interessato
(Capo III)

- ad essere informato sulle finalità del trattamento;
- di fornire e revocare il consenso;
- all'accesso ai propri dati;
- alla rettifica, alla limitazione, alla cancellazione;
- alla portabilità;
- di opposizione al trattamento;
- di presentare un reclamo.

Liceità del trattamento
(Art. 6)

Un trattamento di dati personali è lecito se:

- consenso
- esecuzione contratto
- obbligo legale
- salvaguardia interessi vitali
- compito di interesse pubblico
- perseguimento legittimo interesse titolare

Liceità del trattamento

Un trattamento di dati personali è lecito se:

- ✓ consenso;
- ✓ esecuzione contratto;
- ✓ obbligo legale;
- ✓ salvaguardia interessi vitali;
- ✓ compito di interesse pubblico;
- ✓ perseguimento legittimo interesse del Titolare.

Il rispetto delle regole

Rischi e opportunità

Le Società non possono operare senza trattare dati personali e, nel farlo, devono attenersi a quanto richiesto dalla normativa.

Il mancato rispetto delle regole in materia di protezione dei dati può comportare:

- **Blocco** dei dati / **cancellazione** / **furto** / **utilizzo illegale** – (HR, clienti, fornitori, etc.).
- Attenzione dei media – **danni alla reputazione** della Società e dei dipendenti.
- **Danni agli interessati** o alla comunità.
- **Sanzioni penali** ed amministrative.

Sanzioni interdittive e amministrative previste dal GDPR

Le Società non possono operare senza trattare dati personali e, nel farlo, devono attenersi a quanto richiesto dalla normativa.

Sanzioni e misure interdittive

- Avvertimenti e ammonimenti
- Ingiunzioni, prescrizioni e ordini
- Revoca di certificazioni
- Ordini di sospensione dei flussi di dati verso terzi

Sanzioni amministrative/pecuniarie

- Fino a € 10.000.000 o, per le imprese, fino al 2 % del fatturato mondiale, se superiore
- Fino a € 20.000.000 o, per le imprese, fino al 4 % del fatturato mondiale, se superiore

Sanzioni penali previste dal codice Privacy

	Reclusione fino a 3 anni	Reclusione fino a 3 anni	Reclusione fino a 4 anni	Reclusione fino a 6 anni
	Trattamento illecito	Falsità nelle dichiarazioni al Garante ed interruzione dell’esecuzione dei compiti o dell’esercizio dei poteri del Garante	Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala	Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala

Cosa devono fare le organizzazioni

Check list

- Registro
- Informativa/consensi (Minori / Vulnerabili)
- Nomina interne / esterne
- Formazione e piano formativo
- Profilazione e relativa comunicazione
- DPIA per valutazione rischi
- Procedura di data retention
- Comunicazione a terzi di dati
- Piattaforme tecnologiche, e relativa nomina
- Procedura IT
- Procedura soggetti interessati

La responsabilità del Titolare e l’approccio risk based

Il Regolamento promuove la responsabilizzazione (accountability) dei Titolari del trattamento e l’adozione di approcci e politiche che tengano conto costantemente del rischio che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati.

Privacy by design

Fin dall’ideazione e progettazione di un trattamento o di un sistema, dovranno essere applicate misure tecniche (es. cifratura, pseudonimizzazione) ed organizzative adeguate a tutelare i diritti degli interessati e a gestire possibili problematiche.

Privacy by default

Per impostazione predefinita le organizzazioni dovranno trattare solo i dati personali necessari per le finalità previste e solo per il periodo strettamente necessario.

Informative

Tipologie di informative e moduli per la raccolta e gestione dei consensi:

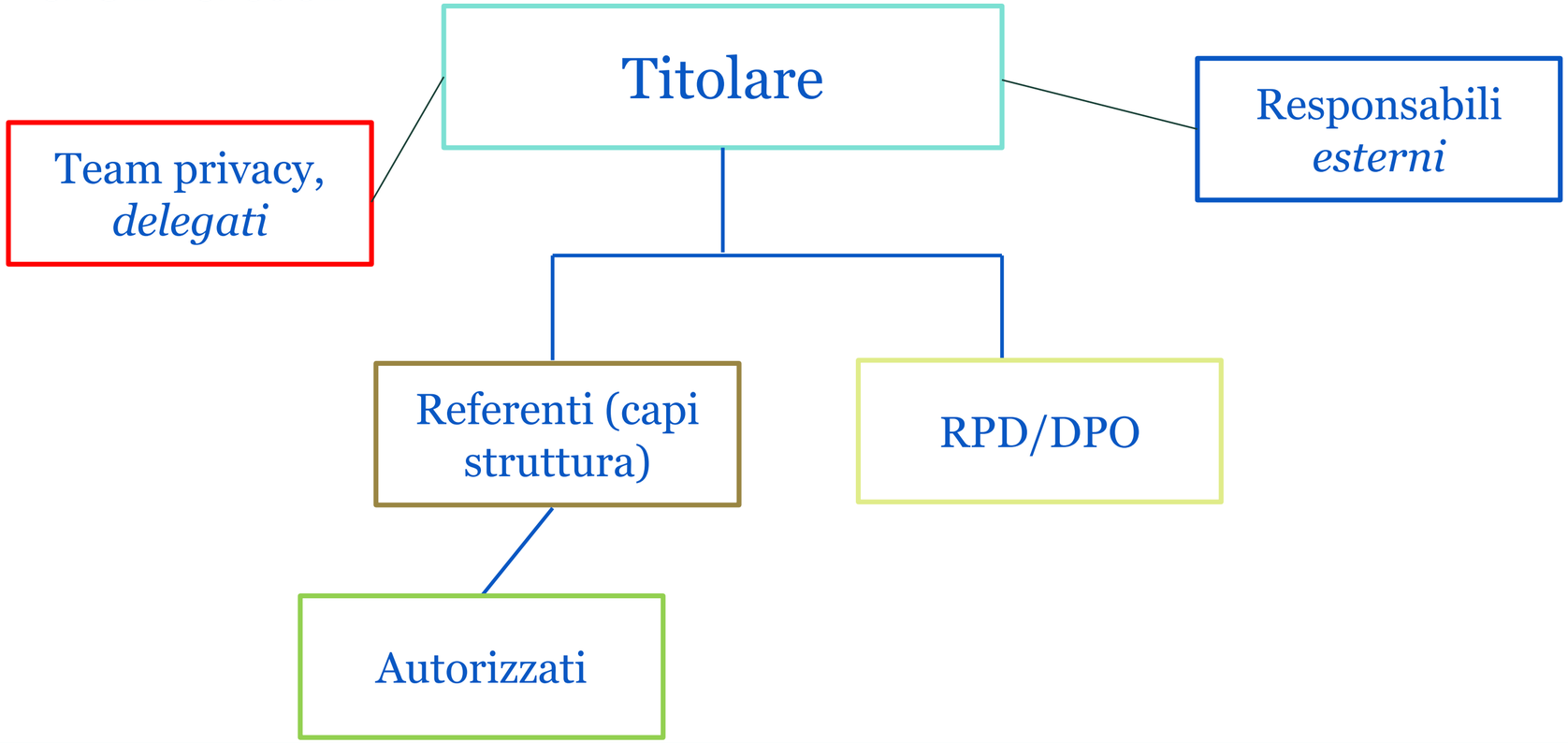
- ✓ informativa dipendenti
- ✓ informativa candidati;
- ✓ informativa utenti;
- ✓ liberatoria privacy generale e liberatoria privacy minorenni;
- ✓ informativa visitatori;
- ✓ informativa videosorveglianza;
- ✓ informativa contrattuale;
- ✓ informative specifiche.

Nomine

Tipologie di nomine che definiscono i rapporti fra le figure coinvolte nel trattamento dei dati:
:

- ✓ nomina del DPO;
- ✓ nomina a responsabile esterno;
- ✓ nomina a soggetto autorizzato;
- ✓ nomina ad Amministratore di sistema;
- ✓ nomina a soggetto autorizzato alla videosorveglianza;
- ✓ altre casistiche specifiche.

Le figure coinvolte nel trattamento dei dati

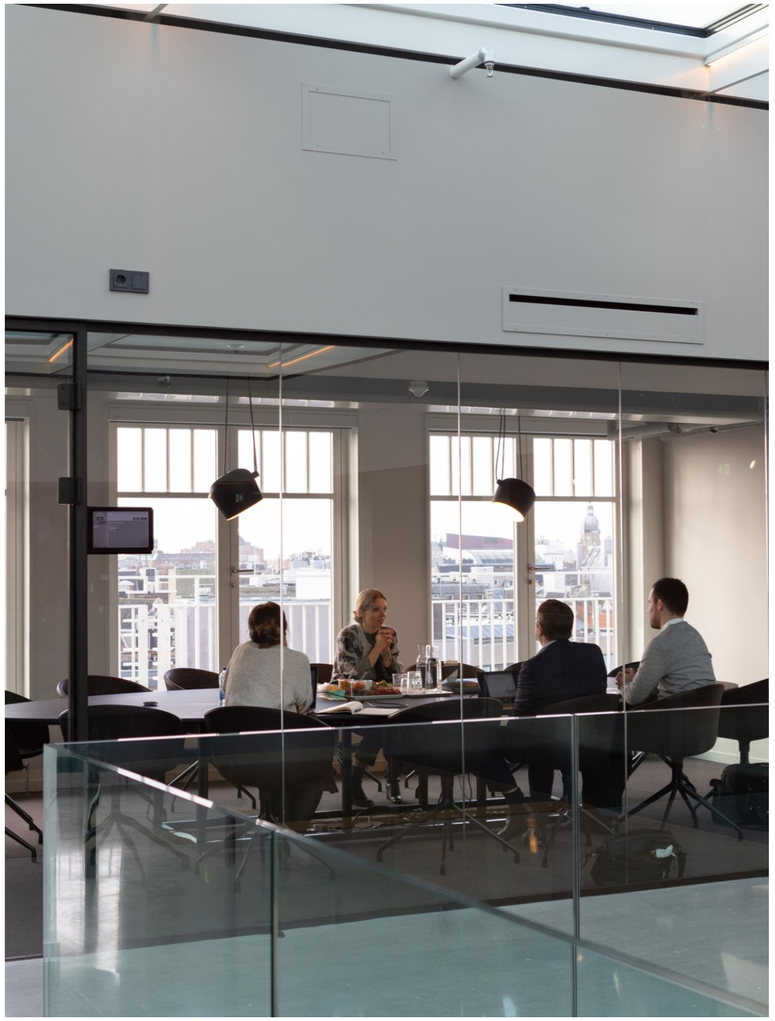


Obblighi specifici per i soggetti autorizzati

Soggetto autorizzato: persona fisica dell'organizzazione che è **autorizzata** a trattare i dati personali.

Obblighi:

- conoscere chi è il Titolare e/o il Responsabile interno del trattamento dati;
- conoscere quali **trattamenti** (azioni) sono stati autorizzati (autorizzazione e istruzioni al trattamento dovrebbero essere scritte);
- **non oltrepassare i limiti** dell'autorizzazione ricevuta e interrogare chiunque chieda di superarli;
- mantenere **elevati standard etici** durante il trattamento dei dati;
- trattare sempre i dati personali come **informazioni riservate**.



Compiti del Responsabile Protezione Dati – RPD (art. 39)

- **informare** e **fornire consulenza** al Titolare o al Responsabile, nonché ai dipendenti che effettuano il trattamento in merito agli obblighi di cui al Regolamento e di cui ad altre disposizioni di legge applicabili in materia;
- **sorvegliare** l'osservanza del Regolamento e delle altre disposizioni di legge, comunitaria o nazionale, in materia di protezione dei dati, nonché delle politiche del titolare (ma non è personalmente responsabile in caso di inosservanza);
- **fornire assistenza** al Titolare nella «valutazione d'impatto»;
- **cooperare** con l'autorità di controllo e fungere da punto di contatto con quest'ultima per le questioni relative al trattamento dei dati personali.

Principi del rapporto con la terza parte

- nomina del fornitore quale Responsabile (data processor) da parte del Titolare;
- istruzioni scritte sulla scopo e sulla natura del processo e sui limiti all'utilizzo dei dati;
- garanzia sulle competenze degli addetti allo svolgimento delle attività contrattuali e vincoli legali;
- diritto di audit da parte del Titolare;
- divieto/Limitazioni al sub-appalto senza espresso consenso e senza le opportune garanzie (contratto scritto con il sub-appaltatore che impone gli stessi obblighi già in capo al fornitore di servizi);
- obbligo di rispettare le misure di sicurezza di legge;
- obbligo di notificare qualsiasi violazione alla sicurezza ed obbligo di cooperare nella risoluzione dei problemi (clausola di risoluzione in caso di violazione).

Procedure

Tipologie di procedure

- ✓ procedura sul trattamento dei dati personali in formato cartaceo, on going;
- ✓ procedura sulla sicurezza informatica, on going;
- ✓ procedura di gestione dei diritti degli interessati;
- ✓ procedura di gestione dei data breach;
- ✓ procedura di data retention, on going;
- ✓ procedure IT.

Ulteriori adempimenti

Tipologie di registri

- ✓ registro dei trattamenti con valutazione del rischio;
- ✓ registro dei trattamenti effettuati dal responsabile esterno;
- ✓ registro dei data breach;
- ✓ eventuali prontuari.

Dpia

- ✓ Videosorveglianza

Il Registro Trattamento Dati (Art. 30)

Il registro indica le effettive mansioni dei soggetti autorizzati al trattamento

- nome del Data Base e owner del sistema;
- descrizione e finalità del trattamento;
- base legale del trattamento (consenso, contratto, etc.)
- descrizione delle categorie di interessati e dei dati personali trattati;
- categorie di destinatari cui i dati sono o saranno comunicati (compresi i Paesi terzi);
- scopo del trasferimento verso un Paese terzo, e la documentazione delle garanzie adeguate;
- termini ultimi previsti per la cancellazione delle diverse categorie dei dati;
- descrizione generale delle misure di sicurezza tecniche ed organizzative;
- server di riferimento ed eventuali archivi.

Valutazione di impatto – DPIA (art. 35)

Obbligatoria quando il trattamento può presentare un elevato **rischio per i diritti e le libertà delle persone fisiche**.

La valutazione d'impatto DEVE ESSERE ESEGUITA prima di procedere al trattamento QUANDO:

- il trattamento consiste in una **valutazione sistematica e globale di aspetti personali** relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche (es. marketing con mezzi automatizzati);
- si effettua un **trattamento, su larga scala**, di categorie particolari di dati personali («sensibili» o «giudiziari»); o
- il trattamento consiste nella **sorveglianza sistematica** su larga scala di una zona accessibile al pubblico (es. videosorveglianza in luoghi pubblici).

Howden Assiteca Consulting

Istruzioni per la compilazione del registro

Registro dei trattamenti (dati essenziali)

Nome del DB e owner del sistema

- Individuare il ruolo dell’Università:
  - ✓Titolare del trattamento;
  - ✓Responsabile del trattamento;
- Nome del DB per poterlo riconoscere e mappare

Registro dei trattamenti (dati essenziali)

Descrizione e finalità del trattamento

- Descrizione del trattamento, in modo da spiegare in maniera sintetica cosa viene fatto e come;
- Scopo del trattamento, a cosa serve raccogliere e trattare i dati.

Registro dei trattamenti (dati essenziali)

Base legale del trattamento

- Individuare la base giuridica che giustifica tale trattamento:
  - ✓ Consenso specifico a una singola finalità;
  - ✓ Esecuzione di contratto o misure precontrattuali;
  - ✓ Obbligo di legge;
  - ✓ Interessi vitali della persona interessata o di un terzo;
  - ✓ Legittimo interesse, prevalente del Titolare;
  - ✓ Compito di interesse pubblico o connesso all'esercizio di pubblici poteri.

- Descrizione dei dati personali che vengono trattati nello specifico trattamento
- Importante ragionare su quelli essenziali e che effettivamente servono

Howden Assiteca Consulting

Registro dei trattamenti (dati essenziali)

Descrizione delle categorie di interessati e dei dati personali trattati

- Origine dei dati (se direttamente soggetto interessato o terzi, e indicarli);
- Modalità del trattamento (cartaceo / elettronico);
- Descrizione dei dati personali che vengono trattati nello specifico trattamento

Importante ragionare su quelli essenziali e che effettivamente servono.

Registro dei trattamenti (soggetti)

Categorie di destinatari cui i dati sono o saranno comunicati (compresi i Paesi terzi)

- Categorie
  - ✓Titolari
  - ✓coTitolari (previa verifica con l’ufficio privacy)
- Indicazione del DPO;
- Indicazione dei Responsabili e Sub-Responsabili del trattamento

Check dell’ufficio privacy sulla nomina e sul trasferimento extra UE.

Registro dei trattamenti (trasferimenti e comunicazione)

Scopo del trasferimento verso un Paese terzo, e la documentazione delle garanzie adeguate

- Indicare se prevista la diffusione;

- segnalare eventuale comunicazione e trasferimento all’estero:

  ✓ intra UE

  ✓ extra Ue

  e in questo caso le garanzie che lo permettono.

Registro dei trattamenti (misure di sicurezza)

Descrizione generale delle misure di sicurezza tecniche ed organizzative

- Specifiche

  ✓ Elenco generale misure di sicurezza con indicazione puntuale

- Trasversali

  ✓ Adottate su tutte le attività di trattamento, inserite dal team privacy con ufficio IT (valgono per tutte, anche per le passate e ancora presenti)

Registro dei trattamenti (altre informazioni)

Termini ultimi previsti per la cancellazione delle diverse categorie dei dati, e luoghi di conservazione

- Termine ultimo di cancellazione,

scelta vincolata con campo aperto di descrizione;

- Applicativi,

scelta vincolata;

- Luoghi fisici,

valutare se tenerlo aperto per maggior possibilità dell’utente di indicare con precisione i luoghi fisici;

- Componenti IT,

campo in valutazione.

Registro dei trattamenti (stima del rischio e pre assessment)

Valutazione del rischio

- Necessario o meno svolgere una valutazione d’impatto, con analisi del rischio (art 29):

✓ Rischio potenziale per i diritti e le libertà degli interessati;

✓ Due criteri “si” rischio alto, uno è medio, zero è basso.

- Pre assessment dpia (art 35):

✓ Si valuterà se obbligatoria o non obbligatoria.

Howden Assiteca Consulting

Case Study

Case study di registro del trattamento

9 luglio:

- Gestione del personale
- Gestione segnalazioni whistleblowing

10 luglio:

- Gestione dei progetti di ricerca
- Gestione del personale

howdengroup.com