IL TRATTAMENTO DEI DATI

Autore/i: Avv. Stefano Rotondo, Gennaro Viggiano

Accettato da: A.S.D. Circolo Nautico Posillipo

STORICO DELLE REVISIONI			
Vers.	**Data di rilascio**	**Motivo della revisione**	**Autore**
	2025	Prima versione	Avv. Stefano Rotondo, Gennaro Viggiano
L'ultima revisione sostituisce qualsiasi revisione precedente.			

PROCEDURA PER LA GESTIONE DEI DATI E DEL LORO TRATTAMENTO

CAPITOLO 1
AMBITO DI APPLICAZIONE

❖ OBIETTIVO DELLA PROCEDURA

Il presente documento descrive le regole, adottate dal Titolare, per la gestione delle informazioni e dei trattamenti classificati, con particolare riguardo ai dati personali ai sensi del GDPR.

Obiettivo della presente procedura è quello di indirizzare la tutela delle informazioni relative ai dati personali trattate dal Titolare, al fine di proteggerle a prescindere dall'origine, dal supporto o dalla fase di elaborazione.

Le linee guida descritte all'interno del presente documento sono da considerarsi misure minime la cui attuazione si rende necessaria per contenere, entro limiti accettabili, il rischio di compromissioni della riservatezza, integrità e disponibilità delle informazioni e dei trattamenti di dati personali effettuati dal Titolare.

In tal senso, queste costituiscono i requisiti di base che devono essere rispettati e che, in quanto tali, in virtù delle specifiche caratteristiche del contesto operativo cui si applicano, possono essere incrementati nei casi in cui siano richiesti livelli di protezione più elevati.

❖ AMBITO DI APPLICAZIONE

Gli indirizzamenti definiti nel presente documento si applicano:

- ai trattamenti di dati personali ai sensi del GDPR effettuati presso le strutture del Titolare;
- a tutti gli asset a supporto dei suddetti trattamenti.

Si precisa, inoltre, che la classificazione delle informazioni oggetto di questo documento si riferisce esclusivamente alla salvaguardia dei diritti e delle libertà dell'interessato ai sensi del GDPR.

❖ RUOLI E RESPONSABILITÀ

1) Titolare del trattamento

- Determina finalità e mezzi del trattamento (art. 4.7 GDPR).
- Approva politiche/procedure privacy e il registro dei trattamenti.
- Nomina per iscritto i Responsabili esterni (art. 28 GDPR) grazie al supporto del Delegato.
- Garantisce misure tecniche/organizzative adeguate (art. 24 e 32) e la gestione dei data breach (artt. 33 – 34).
- Vigila sull'operato di delegati, responsabili e autorizzati.

2) Delegato alla titolarità

- Riceve delega formale con ambito, poteri e limiti.
- Implementa operativamente le decisioni del Titolare (es. approvazione informative standard, check list DPIA, piani di formazione).
- Coordina i referenti di funzione e verifica l'applicazione delle misure nei processi.
- Interfaccia operativa verso DPO e Responsabili esterni.

3) Autorizzati/Incaricati del trattamento (personale interno e collaboratori)

- Operano su istruzioni documentate del Titolare/Delegato (art. 29).
- Trattano i dati nel rispetto delle misure di sicurezza e delle policy istituzionali.
- Segnalano tempestivamente errori, accessi/ricezioni indebite, incidenti o non conformità (es. possibile data breach).
- Mantengono la riservatezza (impegni di confidenzialità/NDA).

4) Responsabili esterni del trattamento (art. 28 GDPR)

- Trattano i dati per conto del Titolare sulla base di contratto/atto giuridico che:
  - descrive oggetto, durata, natura e finalità del trattamento, categorie di dati e interessati;
  - impone misure tecniche/organizzative adeguate, sub-fornitura regolata, supporto a esercizio diritti/DPIA/data breach;
  - disciplina restituzione/cancellazione dati a fine rapporto e audit/monitoraggi.
- Informano senza ritardo il Titolare in caso di violazione di dati personali e collaborano alle attività di risposta.

5) DPO – Data Protection Officer (qualora nominato)

- Funzione di consulenza, sorveglianza e punto di contatto tra il Titolare e gli interessati (art. 39):
  - informa e consiglia Titolare/Responsabili/Autorizzati;
  - verifica l'adeguatezza organizzativa e il rispetto del GDPR/policies;
  - supporta su DPIA e sulle misure correttive;
  - è punto di contatto per interessati e Autorità di controllo.
- **Non** decide al posto del Titolare né sostituisce le valutazioni rimesse alla titolarità.

7) Utilizzatore dell'informazione (chi accede ai dati per esigenze di ruolo)

- Usa i dati solo per le finalità autorizzate e nel perimetro del proprio profilo di accesso.
- Rispetta etichettatura/classificazione, conserva e trasmette i dati con le cautele richieste dal livello.
- Segnala al responsabile della classificazione eventuali errori, incongruenze o ricezioni non attese.

8) Tutti i dipendenti e collaboratori

- Rispettano la presente procedura e le istruzioni ricevute; partecipano alla formazione obbligatoria.
- Segnalano a Titolare/Delegato e, ove nominato, al DPO, scostamenti o casi dubbi.
- Le violazioni possono comportare provvedimenti disciplinari e/o azioni legali.

CAPITOLO 2
DEFINIZIONI E NORME DI RIFERIMENTO

CAP. 2

❖ ACRONIMI E ABBREVIAZIONI

DPO	Data Protection Officer – Responsabile della Protezione dei Dati
EDPB	European Data Protection Board – Comitato europeo per la Protezione dei Dati. Organismo europeo indipendente il cui scopo è garantire un'applicazione coerente del GDPR.
ENISA	European Union Agency for Network and Information Security
GDPR	General Data Protection Regulation – Regolamento Generale sulla Protezione dei Dati, n. 2016/679
IT	Information Technology
WP29	Working Group 29: gruppo istituito ai sensi dell'art. 29 della direttiva 95/46 CE. Dal 25 Maggio 2018 prende il nome di European Data Protection Board.

❖ DEFINIZIONI

Archivio	Qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico (art. 4, n. 6, GDPR).
Autenticazione informatica	L'insieme degli strumenti elettronici e delle procedure per la verifica, anche indiretta, dell'identità dell'utente.

Autorità Garante per la Protezione dei Dati Personali	Autorità istituita dalla legge 31 dicembre 1996, n. 675. Ha sede a Roma.
Banca dati	Qualsiasi complesso organizzato di dati (archivio informatico), riguardanti uno stesso argomento o più argomenti correlati tra loro, strutturato in modo tale da consentire la gestione dei dati stessi (l'inserimento, la ricerca, la cancellazione ed il loro aggiornamento) da parte di un'applicazione, ripartito in uno o più elaboratori elettronici (ad es. server, postazioni lavorative, ecc.) dislocati all'interno della rete LAN del Titolare.
Cancellazione sicura	Modalità di cancellazione che consiste nell'eliminazione irreversibile dei dati contenuti in un supporto elettronico in modo che essi non siano più accessibili a terzi o risultino comunque inintelligibili impedendo così il recupero degli stessi.
Categorie particolari di dati personali	Dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (art. 9, c. 1, GDPR).
Classificazione	L'attribuzione all'informazione di un livello di classificazione ovvero il suo inserimento all'interno di una classe di sicurezza.
Comunicazione	Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del Titolare nel territorio dello Stato, dal Responsabile e dagli Incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Comunicazione elettronica	Ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile.
Consenso dell'interessato	Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento (art. 4, n. 11, GDPR).
Credenziali di autenticazione	I dati e i dispositivi in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.
Dati biometrici	I dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.
Dati genetici	I dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.
Dati personali relativi a condanne penali o reati	Dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza (art. 10 GDPR).
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 (art. 4, n. 1, GDPR).
Declassificazione	La soppressione di qualsiasi menzione di classificazione.
Destinatario	La persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.
Diffusione	Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Documento cartaceo	L'insieme aggregato di informazioni su supporti cartacei.

Documento elettronico	L'insieme aggregato di informazioni su supporti informatici, ovvero file generati attraverso l'utilizzo delle applicazioni informatiche del Titolare.
Incaricato del trattamento	Persona fisica autorizzata a compiere operazioni di trattamento dal Titolare o dal Responsabile.
Informazione	La rappresentazione di dati, atti o fatti rilevanti per il Titolare.
Interessato del trattamento	Persona fisica cui si riferiscono i dati personali.
Minimizzazione dei dati	Ogni Titolare deve trattare solo i dati di cui ha realmente bisogno per raggiungere le finalità del trattamento, nel rispetto dei principi di adeguatezza (proporzionalità rispetto alle finalità) e pertinenza dei dati e limitazione dei trattamenti solo per il raggiungimento delle finalità previste.
Parola chiave	Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.
Profilo di autorizzazione	L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.
Pseudonimizzazione	Il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile (art. 4, n. 5, GDPR).
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 (art. 4, n. 8, GDPR).
Riclassificazione	La ridefinizione del livello di classificazione attribuito all'informazione e, quindi, lo spostamento all'interno di un'altra classe di sicurezza.
Sistema di autorizzazione	L'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.
Sistema informativo	L'insieme di dispositivi, programmi ed infrastruttura di rete.
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 (art. 4, n. 7, GDPR).
Trattamento	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 (art. 4, n. 2, GDPR).
Videosorveglianza	Sistema o dispositivo che permette la visione e la registrazione su supporti singoli, abbinati ad altre fonti o conservati in banche dati di immagini di aree o zone delimitate.
Violazione dei dati personali	Violazione di sicurezza 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, n. 12, GDPR).

❖ NORMATIVA DI RIFERIMENTO

D.lgs. n. 101/2018	Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (GDPR).
D.lgs. n. 196/2003	Decreto Legislativo n. 196 del 30 giugno 2003, contenente il "Codice in materia di protezione dei dati personali", n. c. "Codice Privacy".
Regolamento UE 2016/679	Regolamento 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 e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

Legge n. 300/1970	Statuto dei Lavoratori.
Provvedimento n. 467/2018	Provvedimento dell'Autorità Garante della Protezione dei Dati Personali n. 467 dell'11 ottobre 2018: "Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679".

CAPITOLO 3
PRINCIPI GENERALI DEL TRATTAMENTO

Ogni trattamento di dati personali deve avvenire nel rispetto dei principi fissati dall'art. 5 del GDPR, che qui si ricordano brevemente:

- liceità, correttezza e trasparenza del trattamento, nei confronti dell'interessato;
- limitazione della finalità del trattamento, compreso l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati;
- minimizzazione dei dati: i dati devono essere adeguati pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento;
- esattezza e aggiornamento dei dati, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;
- limitazione della conservazione: ossia, è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
- integrità e riservatezza: occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento.

Il GDPR richiede al titolare di rispettare tutti questi principi e di essere "in grado di comprovarlo" (art. 24).

❖ LICEITÀ DEL TRATTAMENTO

Ogni trattamento deve trovare fondamento in un'idonea base giuridica. I fondamenti di liceità del trattamento di dati personali sono indicati all'art. 6 GDPR: consenso, adempimento di obblighi contrattuali, tutela di interessi vitali della persona interessata o di terzi, adempimento di obblighi di legge cui è soggetto il titolare, tutela di un interesse pubblico o esercizio di pubblici poteri, tutela di un interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati.

Per quanto riguarda le categorie particolari di dati personali, il loro trattamento è vietato, a meno che il titolare possa dimostrare di soddisfare almeno una delle condizioni fissate all'art. 9 GDPR:

- l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche;
- il trattamento è effettuato da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali;
- il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
- il trattamento è necessario per uno dei seguenti scopi:

➢ per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;
➢ per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
➢ per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
➢ per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri;
➢ per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali;
➢ per motivi di interesse pubblico nel settore della sanità pubblica;
➢ per il perseguimento di fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

❖ CONSENSO

Quando il trattamento si fonda sul consenso dell'interessato, il Titolare deve sempre essere in grado di dimostrare che l'interessato ha prestato il proprio consenso, che è valido se:

- all'interessato è stata resa l'informazione sul trattamento dei dati personali;
- è stato espresso dall'interessato liberamente, in modo inequivocabile e, se il trattamento persegue più finalità, è stato espresso specificamente con riguardo a ciascuna di esse. Il consenso deve essere sempre revocabile.

Occorre verificare che la richiesta di consenso sia chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato, per esempio all'interno della modulistica.

Non è ammesso il consenso tacito o presunto. Quando il trattamento riguarda le categorie particolari di dati personali il consenso deve essere esplicito; lo stesso vale per il consenso a decisioni basate su trattamenti automatizzati.

❖ TRASPARENZA DEL TRATTAMENTO

Il Titolare del trattamento deve fornire all'interessato alcune informazioni, anche per metterlo nelle condizioni di esercitare i propri diritti riconosciuti dal GDPR.

L'informativa deve essere fornita all'interessato prima di effettuare il trattamento, quindi prima della raccolta dei dati. Nel caso di dati personali non raccolti direttamente presso l'interessato, l'informativa deve essere fornita entro un termine ragionevole che non può superare un mese dalla raccolta, oppure al momento della comunicazione dei dati (a terzi o all'interessato).

I contenuti dell'informativa sono elencati in modo tassativo dal GDPR. Tra l'altro, il titolare deve sempre specificare i dati di contatto del DPO (qualora nominato), la base giuridica del trattamento, l'eventuale interesse legittimo (se quest'ultimo costituisce la base giuridica del trattamento), nonché se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti. In tutti i casi, il titolare deve specificare la propria identità, le finalità del trattamento, i diritti degli interessati e quali sono i destinatari dei dati. Ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente sono il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di presentare un reclamo all'Autorità Garante per la Protezione dei Dati Personali.

Il Titolare deve porre particolare attenzione alla formulazione dell'informativa, che deve essere soprattutto comprensibile e trasparente per l'interessato, attraverso l'uso di un linguaggio chiaro e semplice.

CAPITOLO 4
IL TRATTAMENTO RESPONSABILE

❖ IL PRINCIPIO DI ACCOUNTABILITY

In base al principio di accountability, il Titolare del trattamento ha il dovere di essere conforme e soprattutto di dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del GDPR. Ha, quindi, il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel Regolamento.

Deve configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili al fine di soddisfare i requisiti del GDPR e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati. Tutto questo deve avvenire prima di procedere al trattamento dei dati vero e proprio e richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili.

❖ RAPPORTI TRA TITOLARE E RESPONSABILE DEL TRATTAMENTO

Il Titolare provvede a designare un responsabile del trattamento, attribuendogli specifici compiti, con un contratto che disciplina tassativamente il trattamento dei dati personali, dimostrando che il responsabile fornisce garanzie sufficienti sulle finalità del trattamento e sulle misure tecniche ed organizzative attuate.

Ogni trattamento affidato a fornitori deve essere regolato da un contratto conforme all'art. 28 GDPR che definisce:

- oggetto, finalità e durata;
- misure di sicurezza;
- limiti alla subfornitura;
- assistenza in caso di esercizio dei diritti o di data breach;
- restituzione/cancellazione dati.

❖ REGISTRO DEI TRATTAMENTI

Il Registro costituisce lo strumento centrale per documentare e gestire la conformità privacy del titolare.

Funzione del Registro:

- censire tutti i trattamenti effettuati;
- verificare basi giuridiche, finalità e categorie di dati;
- definire misure di sicurezza adeguate;
- stabilire tempi di conservazione;
- individuare necessità di DPIA;
- dimostrare la conformità al Garante (accountability).

Il Registro è la base di tutto il sistema privacy e deve sempre riflettere i trattamenti realmente in essere.

Per ciascun trattamento sono riportati:

- finalità;
- categorie di dati e interessati;
- basi giuridiche;
- destinatari o categorie di destinatari;
- trasferimenti extra UE;
- tempi di conservazione;
- misure di sicurezza tecniche e organizzative;
- responsabile di processo;
- fornitori coinvolti.

Il Registro viene aggiornato:

- almeno una volta l'anno;
- ogni volta che nasce, si modifica o termina un trattamento;
- quando cambiano tecnologie, basi giuridiche, finalità, fornitori.

Il Registro è conservato in formato digitale, in luogo sicuro e accessibile solo ai soggetti autorizzati.

❖ DPIA – VALUTAZIONE D'IMPATTO

La DPIA (Data Protection Impact Assessment) è uno strumento obbligatorio di analisi e gestione del rischio privacy quando un trattamento di dati personali può presentare un rischio elevato per i diritti e le libertà degli interessati.

Serve a:

- mappare in dettaglio il trattamento (chi fa cosa, con quali dati, per quali finalità, con quali sistemi);
- valutare se il trattamento è necessario e proporzionato rispetto agli obiettivi istituzionali;
- individuare i rischi per le persone fisiche (non per il titolare in sé);
- definire misure di sicurezza e garanzie (tecniche, organizzative e legali) per ridurre quei rischi a un livello accettabile;
- documentare le valutazioni effettuate dal Titolare, dimostrando la propria accountability.

Non è un esercizio teorico: è un documento operativo che deve guidare come il trattamento viene progettato e gestito.

La DPIA deve:

- descrivere i trattamenti;
- valutare necessità e proporzionalità;
- analizzare rischi per i diritti degli interessati;
- individuare misure per mitigare tali rischi.

Una DPIA deve essere pianificata e segue di norma queste fasi:

- Identificare il trattamento da analizzare (o il progetto/sistema);
- Coinvolgere:
    - Titolare / Delegato alla titolarità,
    - Responsabili del processo interno (es. IT, HR, Marketing),
    - Responsabili esterni critici (es. fornitore software),
    - DPO (se nominato, il suo coinvolgimento è obbligatorio come consulenza).

In particolare, la DPIA deve descrivere i trattamenti in modo chiaro e concreto:

- Finalità (perché trattiamo i dati?);
- Categorie di interessati (dipendenti, clienti, utenti, visitatori, ecc.);
- Categorie di dati (identificativi, di contatto, dati sanitari, immagini, ecc.);
- Flussi (come vengono raccolti, dove transitano, dove vengono conservati, a chi sono comunicati);
- Sistemi e tecnologie utilizzate (software, app, dispositivi, cloud, telecamere, ecc.);
- Ruoli privacy (Titolare, Responsabili esterni, eventuali contitolari);
- Durata del periodo di conservazione;
- Trasferimenti extra UE, se ci sono.

Questa parte è collegata (e deve essere coerente) con il Registro dei trattamenti.

La DPIA, inoltre, deve valutare necessità e proporzionalità del trattamento:

- Il trattamento è davvero necessario per raggiungere gli obiettivi dichiarati?
- Ci sono alternative meno invasive (meno dati, minore frequenza, pseudonimizzazione…)?
- Si rispettano i principi di:
    - minimizzazione dei dati (raccolgo solo ciò che serve),
    - limitazione della finalità (uso i dati solo per gli scopi dichiarati),
    - limitazione della conservazione (non tengo i dati più del necessario),
    - privacy by design e by default (predispongo impostazioni “privacy-friendly” fin dall’inizio).

❖ MISURE DI SICUREZZA

Il Titolare del trattamento deve adottare misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio del trattamento (con l’obiettivo di evitare la distruzione accidentale o illecita, la perdita, la modifica, la rivelazione e l’accesso non autorizzato ai dati personali).

Fra tali misure, il GDPR menziona, in particolare, la pseudonimizzazione e la cifratura dei dati; misure per garantire la riservatezza, l’integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; misure atte a garantire il tempestivo ripristino della disponibilità dei dati; procedure per verificare e valutare regolarmente l’efficacia delle misure di sicurezza adottate.

❖ NOTIFICA DI UNA VIOLAZIONE DEI DATI PERSONALI

Il Titolare del trattamento ha l’obbligo di notificare al Garante le violazioni di dati personali di cui venga a conoscenza, entro 72 ore e comunque senza ingiustificato ritardo, se ritiene probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati.

Nel caso in cui la violazione dei dati personali avvenga al Responsabile del trattamento, l'art. 33 co. 2 GDPR sancisce che il Responsabile del trattamento dovrà informare il Titolare senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione. La notifica all'Autorità Garante dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta al titolare. Se la probabilità di tale rischio è elevata, si dovrà informare della violazione anche gli interessati, sempre senza ingiustificato ritardo.

In ogni caso, è ora obbligatorio documentare le violazioni di dati personali subite, anche se non notificate all'Autorità Garante e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati. Tale documentazione, su richiesta, dovrà essere mostrata al Garante in caso di accertamenti.

❖ RESPONSABILE DELLA PROTEZIONE DEI DATI

La designazione di un Responsabile della Protezione dei Dati (DPO) è finalizzata a facilitare l'attuazione della normativa da parte del Titolare. Fra i compiti del DPO, infatti, rientrano la sensibilizzazione e la formazione del personale e la sorveglianza sullo svolgimento della valutazione di impatto, oltre a fungere da punto di contatto per gli interessati e per il Garante rispetto a ogni questione attinente all'applicazione del GDPR.

❖ I DIRITTI DEGLI INTERESSATI

Il Titolare deve rispettare le modalità previste per l'esercizio di tutti i diritti da parte degli interessati, stabilite nel GDPR.

In primo luogo, il titolare del trattamento deve agevolare l'esercizio dei diritti da parte dell'interessato, adottando ogni misura (tecnica e organizzativa) a ciò idonea. Benché sia il solo titolare a dover dare riscontro in caso di esercizio dei diritti, il responsabile del trattamento è tenuto a collaborare con il titolare ai fini dell'esercizio di tali diritti.

Il Titolare ha il diritto di chiedere informazioni necessarie a identificare l'interessato, e quest'ultimo ha il dovere di fornirle, secondo modalità idonee.

Il termine per la risposta all'interessato è, per tutti i diritti, pari a un mese, estendibile fino a tre mesi in casi di particolare complessità; il Titolare deve comunque dare un riscontro all'interessato entro un mese dalla richiesta, anche in caso di diniego.

La risposta fornita all'interessato non deve essere solo intelligibile, ma anche concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.

CAPITOLO 5
PROCEDURE PRIVACY

CAP. 5

Il titolare deve adottare un sistema integrato di procedure operative per garantire la corretta applicazione del GDPR e assicurare tracciabilità, coerenza e conformità in tutte le attività di trattamento.

Le procedure sono necessarie perché:

- trasformano gli obblighi del GDPR in azioni operative;
- definiscono cosa devono fare dipendenti e responsabili di processo;
- riducono errori e comportamenti non conformi;
- garantiscono che il titolare possa dimostrare il rispetto degli artt. 24 e 5.2 GDPR (accountability).

❖ PROCEDURA GENERALE DI GESTIONE DEL TRATTAMENTO DEI DATI PERSONALI

Questa procedura:

- definisce istruzioni operative per tutti gli Autorizzati;
- regola raccolta, accesso, modifica, conservazione, cancellazione dei dati;
- stabilisce regole sull'uso dei sistemi informativi, e-mail, cloud e dispositivi;
- integra criteri di minimizzazione, sicurezza e gestione dei flussi informativi.

Necessaria perché costituisce la base operativa di tutte le attività quotidiane ed è richiesta dagli artt. 24 e 32 GDPR.

❖ PROCEDURA DI FORMAZIONE PRIVACY

Stabilisce:

- periodicità annuale;
- contenuti minimi;
- registrazione delle presenze;
- aggiornamenti in caso di nuovi rischi o incidenti.

Necessaria in quanto la formazione, ovvero la sensibilizzazione di tutto il personale, è una misura di sicurezza obbligatoria ex art. 32 GDPR.

Si rappresenta, infine, che eventuali nuove ed ulteriori procedure saranno implementate in base alle necessità riscontrate.