UNIVERSITÀ POLITECNICA DELLE MARCHE

DII
Dipartimento di Ingegneria dell'Informazione

unimc

Il registro dei trattamenti ed il ruolo effettivo del DPO

Corsista: Guido Savelli

Mail: studio.guido.savelli@gmail.com

Settembre 2025

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Premessa

Il registro dei trattamenti rappresenta uno strumento fondamentale per la conformità al GDPR, richiedendo una sinergia efficace tra il Data Protection Officer e il titolare del trattamento.

La collaborazione (nella pratica si potrebbe parlare anche di una vera e propria "sostituzione") del responsabile protezione dati personali con il titolare del trattamento per la redazione del registro dei trattamenti, vede spesso *il DPO operare informalmente come consulente privacy del titolare*, proprio a motivo della mancanza di personale di funzione compliance presso il titolare stesso.

Questa presentazione esplora la funzione del registro dei trattamenti e le modalità di collaborazione titolare/DPO per una gestione ottimale di tale documento.

Il registro dei trattamenti: natura e funzione

Il registro dei trattamenti tra obbligo di tenuta e funzione operativa

Strumento da obbligo normativo

Il Regolamento Generale sulla Protezione dei Dati 679/2016 (GDPR) ha introdotto l'obbligo esplicito di tenere un registro delle attività di trattamento attraverso l'articolo 30, che stabilisce:

- ***Obbligo di tenuta*** per titolari e responsabili (art. 30 par. 1 e 2 GDPR)
- ***Descrizione dettagliata degli elementi costitutivi*** (art. 30 par. 1 e 2 GDPR)
- ***Disponibilità del registro all'autorità di controllo su richiesta*** (art. 30 par. 4 GDPR)

Strumento operativo

Il registro rappresenta non solo un obbligo normativo ma un vero e proprio strumento operativo per dimostrare la conformità al principio di accountability.

- ***Documento per la conformità***

Il registro rappresenta la base essenziale su cui costruire l'intero sistema di gestione della privacy dell'ente/organizzazione. Esso costituisce la prova documentale che tutti i trattamenti avvengono nel rispetto dei principi del GDPR, in particolare liceità, correttezza e trasparenza. Fornisce evidenza del rispetto dei principi fondamentali come minimizzazione, limitazioni delle finalità e della conservazione.

- ***Strumento di governance***

Permette di tracciare le attività in materia di protezione dati, normalmente trattati nelle aree di attività dell'ente, consentendo di identificare i rischi associati al trattamento, facilitando l'implementazione di misure di sicurezza adeguate.

Chi deve avere il registro dei trattamenti

Soggetto	Obbligo di tenuta	Riferimento normativo
Titolari del trattamento	Sempre, salvo eccezioni per PMI	Art. 30, par. 1 GDPR
Responsabili del trattamento	Sempre, per trattamenti svolti per conto di titolari	Art. 30, par. 2 GDPR
Aziende/organizzazioni < 250 dipendenti; professionisti	Esentati, salvo trattamenti non occasionali, ad alto rischio o di dati particolari e/o di dati personali relativi a condanne penali e a reati	Art. 30, par. 5 GDPR
Enti pubblici	Sempre, poiché le PA trattano dati personali per lo svolgimento di compiti di interesse pubblico o connessi all'esercizio di pubblici poteri	Art. 30, par. 1 GDPR

Nonostante le esenzioni previste per le piccole organizzazioni, la tenuta del registro è generalmente raccomandata per tutti come best practice di accountability e come strumento di gestione interna della compliance.

Contenuto minimo del registro (art. 30 GDPR)

Dati del titolare e del DPO (se nominato)	Denominazione e dati di contatto (telefono, mail, PEC);
Finalità del trattamento	Scopi perseguiti dal titolare con il trattamento dei dati;
Categorie di interessati	Tipologie di soggetti i cui dati sono oggetto di trattamento;
Categorie di dati	Tipologie di dati trattati (dati comuni, particolari, dati relativi a condanne e reati);
Categorie di destinatari	Tipologie di soggetti ai quali vengono comunicati i dati trattati;
Trasferimenti verso Paesi Extra-UE	Documentazione di eventuali trasferimenti di dati personali verso paesi terzi;
Periodo di conservazione	Indicazione, ove possibile, dei termini per la cancellazione (e periodo di mantenimento);
Misure di Sicurezza	Descrizione, ove possibile, delle misure tecniche e organizzative adottate.

La struttura definita dall'art. 30 GDPR rappresenta il contenuto minimo obbligatorio (con previsioni al paragrafo 2 per il registro dei responsabili), ma tale documento può includere informazioni aggiuntive utili alla gestione della conformità, come la base giuridica del trattamento (consenso, contratto, obbligo legale, ecc.) o l'analisi dei rischi.

Forma e aggiornamento del registro

Requisiti formali

- Documento interno non soggetto a pubblicazione;
- Forma scritta (modalità cartacea o digitale: preferibile formato digitale per facilitare aggiornamenti);
- Sempre disponibile per ispezioni dell'Autorità Garante.

Aggiornamento continuo

Il registro deve riflettere la situazione attuale dei trattamenti e deve essere aggiornato:

- ad ogni nuovo trattamento;
- quando cambiano le finalità o modalità;
- in caso di revisione delle misure di sicurezza;
- dopo eventi significativi (es. data breach).

Ruoli "gestori" nella protezione dati: panoramica con focus sul DPO

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

I soggetti

Titolare del trattamento

Art. 4 par. 1 punto 7 GDPR

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.

Responsabile del trattamento

Art. 4 par. 1 punto 8 GDPR

La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Responsabile protezione dati o DPO (Data Protection Officer)

Artt. 37,38,39 GDPR

Figura specializzata che sorveglia l'osservanza del GDPR, fornisce consulenza, coopera con l'autorità di controllo e funge da punto di contatto per questioni inerenti al trattamento di dati personali.

Il DPO: nuova funzione prevista dal GDPR

Designazione obbligatoria (Art. 37 GDPR)

La nomina del DPO è obbligatoria nei seguenti casi:

- **Trattamento effettuato da autorità pubbliche o organismi pubblici;**
- Quando le attività principali del titolare (o del responsabile) consistono in **trattamenti che richiedono monitoraggio regolare e sistematico degli interessati su larga scala;**
- Quando le attività principali del titolare (o del responsabile) consistono nel **trattamento, su larga scala, di categorie particolari di dati (ex art. 9 GDPR) o dati relativi a condanne penali e a reati (ex art. 10 GDPR).**

Caratteristiche essenziali

- **Indipendenza nel ruolo** Indipendenza operativa e assenza di conflitti di interesse;
- **Competenza professionale** Competenze giuridiche in materia di protezione dati e conoscenze informatiche e in materia di analisi dei rischi;
- **Capacità di interlocuzione** Capacità di interagire con l'Autorità Garante;
- **Posizione nel ruolo** Possibilità di essere interno o esterno all'organizzazione.

Mansioni principali del DPO (art. 39 GDPR)

Attività di consulenza
Fornire consulenza e indicazioni al titolare e ai dipendenti sugli obblighi derivanti dal GDPR e su altre questioni di protezione dati.

Attività di sorveglianza
Monitorare l'osservanza del GDPR e delle politiche interne, inclusa l'attribuzione delle responsabilità e la formazione del personale.

Attività di cooperazione
Fungere da punto di contatto per l'Autorità Garante, gli interessati e i soggetti interni all'organizzazione per questioni di trattamento.

Attività di pareristica nella valutazione del rischio
Fornire pareri sulla valutazione d'impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento.

Il ruolo del DPO nella redazione del registro

DPO e responsabilità sulla redazione del registro

Ruolo formale

Secondo il GDPR, **il DPO non è formalmente responsabile della redazione del registro dei trattamenti, che rimane un obbligo esplicito del titolare, o del responsabile del trattamento.**

Attività di supporto del DPO

- Fornire consulenza sulla corretta struttura del registro;
- Verificare la completezza delle informazioni raccolte;
- Suggerire miglioramenti per rafforzare la conformità;
- Segnalare incongruenze o criticità nei trattamenti documentati.

Criticità nella redazione del registro: 1) organizzazione del titolare

Problemi di natura informativa

- Inesistenza di circolazione regolare di informazioni tra reparti;
- Presenza di informazioni obsolete o incomplete;
- Difficoltà nel tracciare i flussi di dati;
- Scarsa consapevolezza dei referenti interni;
- Comprensione inadeguata del valore della protezione del dato.

Problemi di natura organizzativa

- Aggiornamento del personale formale ma non sostanziale;
- Mancanza di tempo dedicato dai responsabili di funzione;
- Difficoltà nel coordinamento tra reparti;
- Carenza di risorse dedicate alla compliance;
- Modifiche alla struttura organizzativa non comunicate al DPO;
- Nuovi fornitori che trattano dati non registrati prontamente;
- Cambiamenti nelle procedure operative non documentati;
- Assenza di processi strutturati di revisione.

Criticità nella redazione del registro: 2) conoscenza carente di normativa e principi imposti dal GDPR

Mappatura incompleta delle attività di trattamento

Spesso alcune attività di trattamento sfuggono alla mappatura iniziale, soprattutto quelle meno strutturate o occasionali, creando lacune nel registro. Questo accade frequentemente quando:

- manca un coinvolgimento capillare di tutte le funzioni aziendali;
- non vengono considerate attività svolte da consulenti esterni;
- si trascurano i trattamenti cartacei o manuali.

Errori di classificazione dati

Il non corretto tracciamento nel registro delle categorie di dati trattati e dei destinatari porta anche a valutazioni errate dei rischi e delle misure di sicurezza necessarie. Questo aspetto può verificarsi quando si assiste a:

- sottovalutazione della presenza di dati particolari (ex art. 9 GDPR, già dati sensibili);
- errata individuazione dei destinatari dei dati, specialmente terze parti;
- confusione tra responsabili esterni e titolari autonomi.

Collaborazione "pratica": DPO come privacy advisor

Scenario ideale

Il titolare dispone di una funzione compliance interna che gestisce il registro, mentre il DPO fornisce supporto consulenziale e di verifica.

Realtà operativa

Spesso manca una funzione compliance strutturata. Il DPO assume informalmente il ruolo di consulente privacy operativo, gestendo direttamente il registro.

Impatti pratici

Il DPO finisce per occuparsi dell'intero ciclo: dalla mappatura dei trattamenti alla gestione completa del registro, fino all'implementazione delle misure di sicurezza.

Questa prassi, pur diffusa, può creare tensioni rispetto all'indipendenza che il DPO dovrebbe mantenere.

Rischi della "sostituzione" sistematica DPO-titolare

Erosione dell’autonomia/indipendenza

Quando il DPO redige direttamente il registro, rischia di compromettere la propria indipendenza dovendo poi vigilare su documenti che egli stesso ha creato.

Confusione di ruoli

Può generarsi un'ambiguità sulle responsabilità effettive, con il titolare che abdica al proprio ruolo di responsabilità ultima sulla conformità.

Indebolimento dell’accountability

Il principio cardine di responsabilizzazione viene compromesso quando il titolare non partecipa attivamente alla mappatura e documentazione dei propri trattamenti.

Rischi legali

In caso di verifiche o contenziosi, la delega totale al DPO potrebbe essere vista come un'elusione delle responsabilità da parte del titolare.

Best practice collaborazione DPO-titolare

Definizione di ruoli chiara
Definire formalmente la distinzione tra consulenza del DPO e responsabilità decisionale del titolare.

Metodologia strutturata
Stabilire un processo documentato per la compilazione e l'aggiornamento del registro con responsabilità definite.

Revisione periodica
Programmare riunioni trimestrali di verifica congiunta per analizzare e validare le modifiche al registro.

Approvazione formale
Implementare un processo di validazione esplicita dei contenuti del registro da parte del titolare.

Raccomandazioni

Conservare nel tempo la distinzione di ruoli

Preservare l'indipendenza del DPO distinguendo chiaramente il suo ruolo consulenziale dalla responsabilità decisionale del titolare.

Investire in competenze interne

Sviluppare capacità di gestione privacy all'interno dell'organizzazione per ridurre la dipendenza operativa dal DPO.

Adozione di strumenti digitali

Implementare soluzioni tecnologiche che facilitino la collaborazione mantenendo la separazione di ruoli e funzioni.

Valorizzazione del registro

Considerare il registro non come mero adempimento formale ma come strumento strategico di governance dei dati e mitigazione dei rischi.

La collaborazione efficace tra DPO e Titolare rappresenta un equilibrio delicato ma essenziale per garantire una conformità sostanziale al GDPR, che vada oltre la mera compilazione documentale.

Le corrette procedure di modifica e aggiornamento del registro

La gestione delle modifiche nel registro dei trattamenti

Monitoraggio nuove attività

Implementazione di un sistema di rilevazione precoce per nuovi progetti, processi HR, partnership o acquisizioni che comportano nuovi trattamenti di dati personali (nuove finalità, basi giuridiche, categorie di dati, di interessati, di destinatari, ecc..)

Revisione congiunta

Aggiornamento collaborativo del registro con il coinvolgimento del DPO per valutare l'impatto delle modifiche e garantire la corretta documentazione.

Validazione

Approvazione formale delle modifiche da parte del titolare o suo delegato, con verifica della conformità normativa supportata dal DPO.

Un processo ben definito per la gestione delle modifiche è essenziale per mantenere il registro costantemente aggiornato e accurato, evitando gap di conformità.

Audit periodici sul registro

Procedure di audit interno

Implementazione di controlli sistematici con cadenza annuale per verificare:

- La completezza del registro rispetto ai trattamenti effettivi;
- L'accuratezza delle informazioni riportate;
- La conformità alle prescrizioni normative;
- L'adeguatezza delle misure di sicurezza indicate.

Ruolo del DPO nelle verifiche

Il DPO svolge un ruolo cruciale nell'identificare:

- Criticità o incoerenze nel registro;
- Gap tra pratiche effettive e documentazione;
- Necessità di aggiornamento per nuovi trattamenti.

Feed-back continuo dal titolare

Il titolare fornisce regolarmente aggiornamenti su modifiche organizzative o di processo che possono riflettersi sui trattamenti da documentare.

Strumenti digitali per la gestione del registro

Software di privacy management

Soluzioni specializzate che offrono funzionalità dedicate per la creazione e gestione del registro dei trattamenti, con template preimpostati e funzioni di predisposizione automatiche.

Sistemi di workflow condivisi

Piattaforme collaborative che permettono la condivisione del lavoro tra DPO e vari uffici (es. HR, IT, legale, amministrazione, marketing), con funzionalità di assegnazione task, permessi, notifiche e approvazioni.

Dashboard di stato e alert

Sistemi di monitoraggio che forniscono una visione d'insieme dello stato del registro, con indicatori visivi per trattamenti non aggiornati e alert automatici per scadenze di revisione.

L'adozione di strumenti digitali dedicati semplifica significativamente la collaborazione tra DPO e Titolare, riducendo il rischio di errori e omissioni.

La sintesi dei ruoli nella predisposizione del registro

Predisposizione del framework

Il DPO prepara:

- Template del registro conforme alle best practice;
- Questionari per la raccolta delle informazioni;
- Linee guida per la compilazione;
- Criteri per valutare l'adeguatezza delle misure.

Implementazione da parte del titolare

Il titolare (tramite referenti interni):

- Compila il registro con le informazioni specifiche;
- Consulta il DPO per chiarimenti o dubbi;
- Valida i contenuti finali del registro;
- Approva formalmente il documento completo.

La partecipazione del DPO alla gestione del registro nell'ente locale – un caso pratico

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Esempio pratico: partecipazione del DPO nella gestione del registro trattamenti in un ente locale 1/2

Assistenza del DPO nella rilevazione di asset, procedure, archivi e gestione del cartaceo

- Censimento degli asset dell'ente e dei software utilizzati;
- Mappatura degli archivi fisici e informatici e delle procedure di accesso;
- Analisi dei flussi documentali interni ed esterni.

Focus congiunto DPO/preposti nell'ente su attività di trattamento

Esempi:

- Trattamento gestione risorse umane;
- Trattamento dei servizi sociali e dati sanitari;
- Trattamento sistemi di videosorveglianza comunale;
- Trattamento servizi demografici dell'ente;
- Trattamento servizi lavori pubblici, progettazione, urbanistica ed edilizia residenziale pubblica;
- Trattamento notificazione atti;
- Trattamento gestione protocollo, della posta e dei documenti; pubblicazione atti e gestione albo pretorio;
- Trattamento servizi di gestione contabile e finanziaria dell'ente; servizi tributari.

Esempio pratico: partecipazione del DPO nella gestione del registro trattamenti in un ente locale 2/2

Verifica annuale congiunta

Pianificazione di un audit annuale completo con la partecipazione di:

- DPO e suo team di supporto;
- Segretario comunale o Direttore Generale;
- Responsabili di settore (titolari di Posizioni Organizzative);
- Referenti informatici dell'ente.

Sessioni formative DPO

Programma di formazione a cura del DPO per garantire la corretta gestione del registro:

- Workshop per referenti privacy di sede;
- Illustrazione dei tutorial sull'uso del software di gestione privacy adottato;
- Linee guida per l'aggiornamento autonomo.

Conclusioni

Benefici della collaborazione

Collaborazione DPO/titolare come fondamento della compliance

La sinergia tra DPO e titolare rappresenta il pilastro su cui si costruisce un'efficace sistema di gestione della protezione dei dati personali: solo attraverso una collaborazione strutturata e continua è possibile garantire che il registro rifletta accuratamente la realtà dei trattamenti.

Registro: uno strumento di governance

Il registro dei trattamenti va oltre il semplice adempimento formale, configurandosi come un vero e proprio strumento di governance dei dati. La sua corretta gestione permette di:

- Mappare i flussi informativi dell'organizzazione;
- Identificare preventivamente potenziali rischi;
- Razionalizzare i trattamenti e ottimizzare i processi.

Benefici tangibili

Una gestione collaborativa del registro porta vantaggi concreti in termini di:

- **Trasparenza** verso interessati e autorità;
- **Efficienza** nei processi di compliance:
- **Responsabilizzazione** di tutta l'organizzazione;
- **Riduzione del rischio di sanzioni** e danni reputazionali.