GDPR e ADEMPIMENTI AZIENDALI

Milano, 15 giugno 2023

AVV. ALESSIA NATALONI

Valutazione di impatto (DPIA) e rischio del trattamento

La valutazione di impatto del trattamento (D.P.I.A., cioè Data Protection Impact Assessment) è un processo volto a descrivere il trattamento, valutarne la **necessità e la proporzionalità** e a gestire gli eventuali rischi per i diritti e le libertà delle persone derivanti dal trattamento.

Con tale strumento si sposta l'onere dell'analisi dei rischi dai Garanti ai Titolari del trattamento.
Se prima era necessario richiedere all'Autorità di controllo un'autorizzazione preventiva, adesso il GDPR pone questo onere direttamente a carico del Titolare del trattamento.
Previsto dall'art. 35 GDPR è emanazione diretta del **principio di accountability** (il nuovo quadro normativo è prevalentemente incentrato sui doveri e sulla responsabilizzazione del Titolare del trattamento).
Il Titolare, quale soggetto che determina le finalità e i mezzi del trattamento, nonché le misure di sicurezza, ha maggiore discrezionalità nel decidere come conformarsi alle disposizioni del nuovo Regolamento, ma ha l'onere di dimostrare le ragioni a supporto di tali decisioni e le motivazioni per cui ritiene che le medesime siano compliance con il regolamento.
Con tale valutazione si assicura trasparenza e protezione nelle operazioni di trattamento dei dati personali.

La valutazione del rischio, da realizzare per ogni trattamento dovrà portare il Titolare a decidere in autonomia se sussistono rischi elevati inerenti il trattamento, in assenza dei quali potrà procedere oltre.

Se invece ritenesse sussistenti rischi per le libertà e i diritti degli interessati, dovrà individuare le **misure specifiche** richieste per attenuare o eliminare tali rischi.

Solo nel caso in cui il Titolare non dovesse trovare misure idonee a eliminare o ridurre il rischio, occorrerà consultare l'Autorità di controllo (consultazione preventiva). Normalmente l'Autorità interviene *ex post*, sulle valutazioni del Titolare, indicando le misure ulteriori eventualmente da implementare, fino ad eventualmente ammonire il titolare o vietare il trattamento.

In ogni caso il titolare dovrà giustificare le sue valutazione e rendicontarle, anche eventualmente nel **registro dei trattamenti**.

Contenuto della DPIA

La valutazione di impatto deve contenere almeno:

- la descrizione sistematica dei trattamenti previsti, la finalità del trattamento, compreso la base giuridica;
- la valutazione della necessità e proporzionalità del trattamento in relazione alla finalità;
- la valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste per affrontare i rischi, incluse le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati e dimostrare la conformità al regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Il Titolare e il Responsabile del trattamento provvedono a sviluppare la valutazione di impatto.
La valutazione **implica l'analisi e la descrizione delle aree critiche da esaminare, del profilo di tutti i soggetti coinvolti, gli effetti e le conseguenze del trattamento dei dati, una valutazione dei rischi collegati, e quindi la stesura di un piano di mitigazione dei rischi.**
Il DPO analizzerà il rapporto e proporrà eventuali migliorie. Se il rapporto è approvato si passa all'attuazione delle misure di sicurezza proposte.

Procedura per la DPIA

Di seguito si indicano le fasi generalmente necessarie per completare una DPIA:

- **Raccolta informazioni**;
- **Descrizione dei trattamenti**: descrizione delle finalità, delle categorie di persone e dati coinvolti, della basi giuridiche e valutazione della proporzionalità dei trattamenti.
- **Data Flow**: essenziale è una descrizione del flusso dei dati, utile in formato diagramma, per capire quali problemi possono sorgere e dove è possibile (o necessario) intervenire.
- **Revisione dei principi e dei diritti**: principi del GDPR e diritti dell'interessato devono sempre essere tenuti in considerazione per valutare se e come i trattamenti incidono su di essi.
- **Identificazione dei rischi e conseguente valutazione delle misure per minimizzare o eliminare tali rischi**.
- **Realizzazione del rapporto**: il tutto va documentato in un rapporto.
- **Consultazione preventiva**: nei casi in cui non si riesce a stabilire misure per mitigare i rischi occorre rivolgersi preventivamente all'Autorità di controllo (*prior consultation*).
- **Revisione e firma**: il rapporto finale va sottoposto a revisione dalle parti coinvolte, e poi firmato dal Titolare del trattamento.
- **Implementazione**: il Titolare dovrà porre in essere i suggerimenti emersi dal rapporto (o dalla consultazione del Garante) per minimizzare o eliminare i rischi dei trattamenti.
- **Eventuale pubblicazione**: a fini di trasparenza può essere utile pubblicare il rapporto.

L’articolo 35, comma 3, del GDPR indica alcuni esempi in cui è necessario effettuare la valutazione di impatto ovvero:

a) 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;
b) il **trattamento, su larga scala, di categorie particolari di dati personali** (articolo 9 del GDPR: dati personali che rivelino 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) o di dati relativi a condanne penali e a reati (articolo 10 del GDPR);
c) la **sorveglianza sistematica su larga scala di una zona accessibile al pubblico.**

La conduzione della DPIA è in capo al Titolare del trattamento dei dati, anche se, in concreto, lo svolgimento della valutazione d’impatto può essere affidata ad un consulente esterno.
In caso di soggetto esterno, il Titolare sarà tenuto a monitorare lo svolgimento del Data Protection Impact Assessment, eventualmente consultando anche il responsabile IT e, quando nominato, il Data Protection Officer (DPO) o Responsabile della Protezione dei Dati (RPD).

DPO – Data Protection Officer

Il **DPO** è una figura esperta nella protezione dei dati, il cui compito è **valutare e organizzare la gestione del trattamento di dati personali e dunque la loro protezione, all'interno di un'organizzazione, affinché questi siano trattati in modo lecito.**

Secondo il testo del Regolamento Europeo, una volta designato il responsabile per la protezione dei dati personali, l'organizzazione aziendale deve assicurarsi che sia prontamente coinvolto e che possa adempiere alle sue funzioni in piena indipendenza allo scopo di non creare un conflitto di interessi nello svolgimento del suo compito di vigilanza sull'attuazione e l'applicazione della normativa.
Il Titolare del trattamento sostiene il DPO nel suo ruolo per l'esecuzione dei suoi compiti, fornendogli tutte le risorse necessarie quali risorse finanziarie, personale, locali, attrezzature e quanto necessario per adempiere alle sue funzioni.
A seconda dell'organigramma stabilito dall'azienda o dall'ente, può esserci anche più di un responsabile, specialmente nei casi di grandi organizzazioni e multinazionali, nelle quali la mole di lavoro prevedrebbe l'impiego di più soggetti.

Ai sensi dell'art. 38 del Regolamento europeo sulla protezione dei dati, il DPO:

a. deve essere adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali;
b. deve essere sostenuto dal Titolare del trattamento nell'esecuzione dei compiti assegnati;
c. deve avere le risorse necessarie per adempiere ai compiti assegnati;
d. deve poter accedere ai dati personali e ai trattamenti che riguardano la struttura in cui è inserito;
e. deve mantenere la sua conoscenza specialistica (corsi di aggiornamento);
f. deve essere indipendente nell'esercizio delle sue funzioni;
g. non deve essere penalizzato o rimosso per l'adempimento dei propri compiti;
h. è tenuto al segreto e alla riservatezza in merito all'adempimento dei propri compiti;
i. non può svolgere altre funzioni o compiti che determino un conflitto di interessi.

L'articolo 39 del Regolamento europeo sulla protezione dei dati personali, elenca i compiti del DPO, che sono almeno i seguenti:
a. **informare e consigliare** il titolare del trattamento o il Responsabile nonché i dipendenti;
b. **sorvegliare l'osservanza del Regolamento** e delle altre leggi vigenti nell'Unione Europea in materia nonché delle policy;
c. fornire se richiesto un **parere sulla valutazione di impatto sulla protezione dei dati personali e sorvegliarne lo svolgimento**;
d. **fungere da punto di contatto per l'autorità di controllo** per questioni connesse al trattamento di dati personali.

Il DPO deve essere nominato quando:

a) il trattamento è effettuato da **un'autorità pubblica o da un organismo pubblico.**

b) Le attività principali (cd. core business) del Titolare del trattamento consistono in processi che, per loro natura, ambito di applicazione e/o finalità, richiedono il **monitoraggio regolare e sistematico degli interessati.**

c) Nel caso di trattamento su **larga scala di speciali categorie di dati personali o di dati relativi a reati e condanne penali.**
Il concetto di "larga scala" dev'essere valutato sulla base di alcuni specifici criteri quali, ad esempio, il numero di interessati coinvolti, la durata del trattamento e la sua estensione geografica.
Tra i trattamenti non su larga scala sono invece compresi: il trattamento dei dati di un proprio paziente da parte del medico di famiglia ed il trattamento dei dati personali di natura penale da parte di un avvocato.

Obbligo della formazione in materia privacy

Il Regolamento non specifica nel dettaglio che tipo di corsi devono essere svolti (come ad es. prevede la normativa in materia di sicurezza sul lavoro), ma l'obbligo deriva dagli **artt. 29, 32 e 39** del medesimo Regolamento.

Come previsto dall'art. 29 del Regolamento, il Responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del Titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati **se non è istruito** in tal senso dal Titolare stesso, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Gli obblighi formativi sono introdotti dall'art. 39.1.b del Regolamento, il quale prevede, tra i compiti del DPO, quello di "*sorvegliare l'osservanza […] delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi […] la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo*", ed inoltre, l'art. 32.4 del Regolamento dispone che "*chiunque abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal Titolare del trattamento".*

Le aziende e le Pubbliche Amministrazioni, pertanto, devono implementare dei processi formativi che rispondano ai requisiti delle Misure di Sicurezza: testabili, verificabili e valutabili per chiunque gestisca dati personali.

Il corso PRIVACY ha l'obiettivo di fornire le nozioni principali *per istruire dipendenti* e collaboratori sul tema della protezione dei dati personali ai sensi del Regolamento UE 2016/679 (GDPR), trattando in particolare i seguenti argomenti:

- Principi del Regolamento 2016/679
- Soggetti del trattamento dati personali
- Nomine delle figure in relazione alla struttura organizzativa
- Approccio basato sul rischio del trattamento
- Rispetto delle procedure e delle misure di sicurezza adottate
- Documenti del GDPR

Il mantenimento della **Compliance al GDPR PRIVACY richiede un aggiornamento costante della formazione** per tutti gli addetti che trattano i dati.

In caso di violazione degli articoli 29 e 39 (obbligo formativo), sono previste sanzioni amministrative pecuniarie rilevanti.

Il sistema sanzionatorio

L'art. 83 del GDPR distingue due gruppi di sanzioni amministrative: nel primo gruppo rientrano le violazioni cosiddette di minore gravità, per le quali sono previste le sanzioni amministrative pecuniarie di **importi fino a 10 milioni di euro o, per le imprese (da intendersi come gruppo) fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore,** e riguardano nello specifico le violazioni degli obblighi imposti ai seguenti soggetti:

- **Titolare e Responsabile del trattamento** (artt. 8, 11, da 25 a 39, 42 e 43 GDPR):

- consenso dei minori (art. 8);
- trattamento che non richiede l'identificazione (art. 11);
- principi di privacy by design e by default (art. 25);
- accordo interno per determinare responsabilità tra contitolari (art. 26);
- nomina del rappresentante di titolari o dei responsabili non stabiliti nell'Unione e i suoi compiti (art. 27);
- compiti e responsabilità del responsabile del trattamento (art. 28);
- trattamento da parte dei dipendenti e collaboratori del titolare o del responsabile (art. 29);
- tenuta dei registri delle attività di trattamento (art. 30);
- cooperazione del titolare o del responsabile del trattamento con l'autorità di controllo (art. 31);

- adozione di misure di sicurezza adeguate (art. 32);
- notifica all'autorità di controllo di una violazione di dati personali (art.33);
- comunicazione all'interessato di una violazione di dati personali (art. 34);
- valutazione d'impatto (art. 35);
- consultazione preventiva (art. 36);
- designazione del DPO (art. 37);
- obblighi del titolare e del responsabile nei confronti del DPO (art. 38);
- compiti assegnati al DPO (art. 39);
- obblighi in materia di certificazione (art. 42)

- Organismo di certificazione;

- Organismo di controllo dei codici di condotta (art. 41 GDPR);

Il secondo gruppo di sanzioni, più pesanti in considerazione della maggiore gravità delle fattispecie a cui sono ricondotte, ammontano **fino a 20 milioni di euro o, per le imprese (da intendersi come gruppo), fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore**, e riguardano nello specifico le seguenti violazioni:

- principi generali applicabili al trattamento (art. 5), condizioni di liceità del trattamento (art. 6), condizioni per il consenso (art. 7) e trattamento di categorie particolari di dati personali (art. 9);
- diritti degli interessati (artt. da 12 a 22);
- trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale (artt. da 44 a 49);
- obblighi previsti dalle legislazioni degli Stati membri adottate a norma del capo IX (giornalismo, espressione accademica o letteraria, accesso ai documenti delle PA, rapporti di lavoro, archiviazione nel pubblico interesse, ricerca scientifica, storica o statistica);
- negato accesso all'autorità di controllo durante l'esercizio dei propri poteri di indagine o inosservanza di un suo provvedimento di carattere correttivo.

GRAZIE PER L'ATTENZIONE

LawDeal

Società tra avvocati Law Deal S.a.s.
P.IVA 11210800964

Via Bastioni di Porta Nuova, 21
20121 Milano
Italia

Piazza del Popolo, 18
00187 Roma
Italia

info@lawdeal.it

lawdeal@pec.it