Protezione dei dati personali

Attività formativa Ordini Provinciali

Roma, 13 Aprile 2021

1. **Introduzione**
2. Definizioni
3. Responsabile per la Protezione dei dati personali
4. Adeguamento al GDPR

Agenda

Introduzione

General Data Protection Regulation 679/2016

Regolamento 2016/679/EU

- Carattere di obbligatorietà
- Direttamente applicabile nei Paesi EU

24 maggio 2016: Entrata in vigore nell'UE
25 maggio 2018: Applicazione disposizioni GDPR

D.Lgs. 196/2003:
- Codice In Materia Di Protezione Dei Dati Personali
- Provvedimenti del Garante

D.Lgs. 101 del 10 agosto 2018:
Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 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

D.Lgs. 196/2003 modificato dal D. lgs. 101/2018:
- E' la normativa nazionale attualmente vigente in tema di protezione dei dati personali

NOVITÀ
Introduce nuove indicazioni sulla protezione dei dati personali, rafforzando il principio di responsabilizzazione dei Titolari e Responsabili del Trattamento

OBIETTIVO
Armonizza le attività di trattamento dei dati, in maniera più omogenea e trasparente, così da assicurare la libera circolazione dei dati personali, proteggendo i diritti e le libertà fondamentali delle persone fisiche.

APPLICAZIONE TERRITORIALE
1. Si applica al trattamento di dati personali, effettuato o meno nell'UE, da Titolari o Responsabili dell'UE **2**.Si applica al trattamento di dati personali di interessati dell'UE, da Titolari o Responsabili extra UE che: - offrono beni/servizi, anche gratuitamente - monitorano il comportamento che ha luogo nell'UE

1. Introduzione
2. **Definizioni**
3. Responsabile per la Protezione dei dati personali
4. Adeguamento al GDPR

Agenda

Definizioni

Dati personali

- **Dato personale ex art. 4 GDPR:**

Con l'espressione *dato personale* si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile; 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 ex art. 9 GDPR:
Si tratta dei dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, 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

Dati personali relativi a condanne penali e reati ex art. 10 GDPR:
Si tratta di dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza

Definizioni

Articolo 4 del GDPR

➢ **Interessato**	Persona fisica a cui si riferiscono i dati personali oggetto del trattamento/dei trattamenti, ovvero il proprietario dei suoi dati.
➢ **Trattamento**	Qualsiasi operazione applicata a dati personali, come raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, limitazione, cancellazione o distruzione.
➢ **Titolare del trattamento**	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**	Persona fisica o giuridica, autorità pubblica, servizio od organismo che tratta dati personali per conto del Titolare del trattamento.

*'Il **Responsabile della Protezione dei Dati** (RPD o DPO), Persona fisica designata, dal Titolare o dal Responsabile del trattamento, al monitoraggio del corretto adempimento dei requisiti normativi in tema di Data Privacy e coinvolto ogniqualvolta sia necessario effettuare valutazioni in merito alle attività di trattamento dei dati personali* (in considerazione degli artt. 37 e ss del GDPR)

Definizioni

Articolo 4 del GDPR

➢ **Profilazione**	Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi ad una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.
➢ **Consenso**	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.
➢ **Violazione dei dati personali (Data Breach)**	La 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 trasmessi, conservati o comunque trattati.

*'**Chiunque agisca sotto l'autorità del titolare** del trattamento **o del responsabile** del trattamento, **che abbia accesso a dati personali non può trattare tali dati se non è istruito** in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.'* (art. 29 GDPR impropriamente definito «*incaricato o autorizzato*»)

1. Introduzione
2. Definizioni
3. **Responsabile per la Protezione dei dati personali**
4. Adeguamento al GDPR

Agenda

Responsabile per la Protezione dei Dati

Il ruolo del RPD/DPO

Principali riferimenti normativi

- Artt. 37 e ss. del GDPR «*Designazione, posizione e compiti del Responsabile per la Protezione dei Dati*»

Quando nominarlo

- Il Titolare del Trattamento e il Responsabile del Trattamento designano sistematicamente un Responsabile della Protezione dei Dati (Data Protection Officer) ogniqualvolta:
  - il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico;
  - le attività principali del Titolare o del Responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
  - le attività principali del Titolare o del Responsabile del trattamento consistono nel trattamento, su larga scala.

Compiti ai sensi dell'art. 39 del GDPR

- Informare e fornire consulenza al Titolare del trattamento o al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal regolamento
- Sorvegliare l'osservanza del Regolamento Europeo 679/2016
- Fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati
- Cooperare con l'Autorità di Controllo
- Fungere da punto di contatto per l'Autorità di Controllo per questioni connesse al trattamento

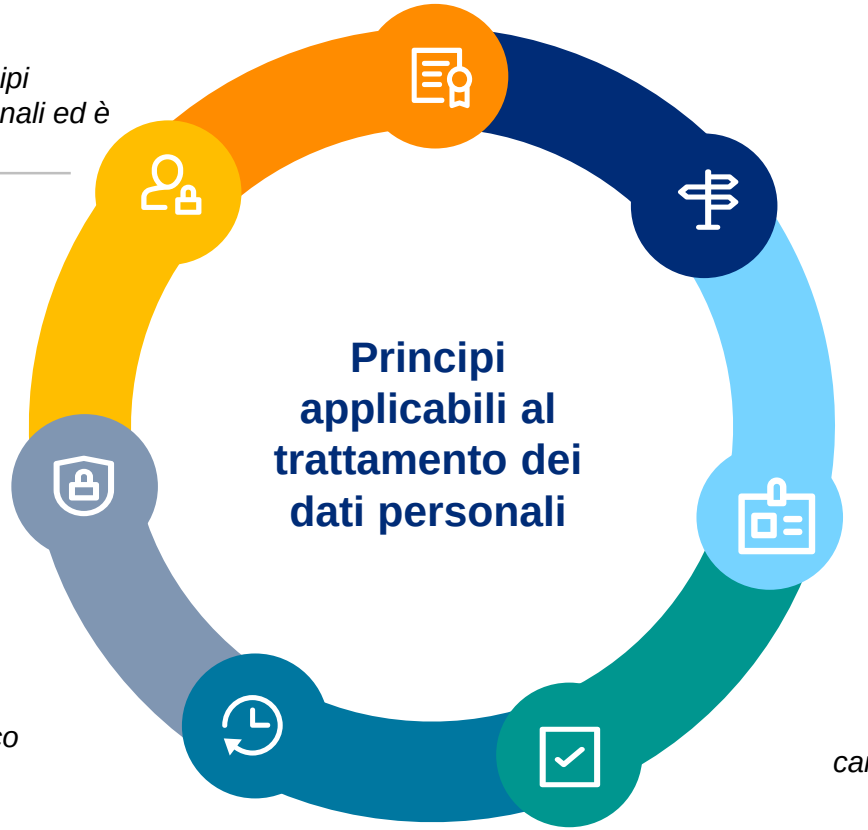
Definizioni

Articolo 5 del GDPR

Liceità, correttezza e trasparenza
trattati in modo lecito, corretto e trasparente nei confronti dell'interessato

Responsabilizzazione
da parte del titolare del trattamento, competente per il rispetto di tutti i principi applicabili al trattamento dei dati personali ed è in grado di comprovarlo

Limitazione della finalità
raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità



Integrità e riservatezza
trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali

Minimizzazione dei dati
adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati

Limitazione della conservazione
conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati

Esattezza
esatti e, ove necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare/rettificare tempestivamente dati inesatti rispetto alle finalità per le quali sono trattati

1. Introduzione
2. Definizioni
3. Responsabile per la Protezione dei dati personali
4. **Adeguamento al GDPR**
5. Documentazione a supporto

Agenda

Adeguamento al GDPR

Informative privacy ai sensi degli art. 13-14 del GDPR

1. Finalità e basi giuridiche del trattamento
2. Dati personali oggetto di trattamento
3. Tempi di conservazione dei dati
4. Modalità d'uso dei dati
5. Ambito di circolazione dei dati
6. Natura del conferimento
7. Diffusione dei dati
8. Trasferimento dei dati all'estero
9. Titolare e Responsabile della Protezione dei dati
10. Esercizio dei diritti
11. Modalità di esercizio dei diritti

*'**La richiesta del consenso** deve essere presentata in modo distinto da altre richieste, **in forma comprensibile e** facilmente **accessibile, utilizzando** un **linguaggio semplice e chiaro**; il **consenso** deve essere **prestato in maniera libera ed espressa**. **L'interessato ha il diritto di revocare** il proprio consenso in qualsiasi momento. La revoca non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Il consenso è revocato con la stessa facilità con cui è accordato.'* (art. 7 GDPR)

Adeguamento al GDPR

Esercizio dei diritti degli Interessati

Principali riferimenti normativi

- Art. 15 del GDPR «*Diritto di accesso*»
- Art. 16 del GDPR «*Diritto di rettifica*»
- Art. 17 del GDPR «*Diritto all'oblio*»
- Art. 18 del GDPR «*Diritto di limitazione del trattamento*»
- Art. 20 del GDPR «*Diritto alla portabilità dei dati*»
- Art. 21 del GDPR «*Diritto di opposizione*»
- Art. 22 del GDPR «*Processo decisionale automatizzato*»

Principali punti d'attenzione

- Attuazione di misure tecniche ed organizzative per favorire e garantire l'esercizio dei diritti ed il riscontro alle richieste presentate dagli Interessati, rispondendo entro 1 mese dalla richiesta pervenuta (anche in caso di diniego), estendibili fino a 3 mesi in caso di particolare complessità

Warning

- In caso di esercizio dei diritti da parte dell'Interessato, a titolo esemplificativo, prevedere le seguenti attività:
  - ✓Ricezione dell'istanza degli Interessati;
  - ✓Comunicazione dell'istanza al DPO o referente interno privacy;
  - ✓Valutazione dell'istanza;
  - ✓Notifica ad eventuali soggetti terzi (ad esempio, Responsabile del trattamento);
  - ✓Elaborazione di una risposta all'Interessato;
  - ✓Archiviazione.

Adeguamento al GDPR

Applicazione del principio di Privacy by Design e Privacy by Default

Principali riferimenti normativi

- Art. 25 del GDPR «*Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita*»

Principali punti d'attenzione

- Limitazione del trattamento ai soli dati necessari al raggiungimento della finalità
- Previsione, già in fase di progettazione, di misure tecniche e organizzative adeguate, a garanzia della protezione dei dati

Warning

- In caso di sviluppo di un nuovo processo / servizio / strumento, o di modifica di uno già esistente che comporta un nuovo trattamento di dati personali o la modifica di un trattamento, comunicarlo al DPO già in fase di progettazione e prima che si effettui il trattamento.

Adeguamento al GDPR

Applicazione del principio di Privacy by Design e Privacy by Default prima del trattamento

1. PERIMETRO TRATTAMENTO DEI DATI

Individuare i dati personali oggetto di trattamento, le operazioni svolte, le finalità, i soggetti interessati.

2. MISURE DI SICUREZZA

Individuare le misure di sicurezza posto / o da porre a protezione dei dati.

3. PRINCIPIO DI MINIMIZZAZIONE DEI DATI

Definire i dati minimi necessari al perseguimento delle finalità e i temi di conservazione (i dati vanno conservati per il minor tempo possibile).

4. NOMINA RESPONSABILE DEL TRATTAMENTO

Individuare i soggetti terzi (es. fornitori) che, per l'erogazione dei servizi tratteranno dati personali del Titolare e procedere, ove opportuno, alla Nomina in qualità di Responsabile del trattamento.

5. UBICAZIONE GEOGRAFICA DEI SERVER

Individuare l'ubicazione geografica dei server sui cui risiedono /transistano temporaneamente i dati personali.

6. ESECUZIONE DPIA

Eseguire la DPIA (se il trattamento può comportare un alto rischio per l'interessato)

7. INFORMATIVE PRIVACY

Valutare il rispetto dei principi di liceità, predisporre idonea inforamtiva privacy e definire la modalità di raccolta dei consensi.

8. AGGIORNAMENTO REGISTRO

Aggiornare il «Registro delle attività di trattamento»

Adeguamento al GDPR

Registro delle attività di trattamento

Principali riferimenti normativi

- Art. 30 del GDPR «*Registri delle attività di trattamento*»

Principali punti d'attenzione

- Obbligo di predisporre il Registro delle attività di trattamento dei dati personali per Titolare e Responsabile (tenuto in forma scritta/elettronica). Il Registro deve essere manutenuto e aggiornato costantemente in modo che i trattamenti risultino allineati con le evoluzioni dell'Ente dl punto di vista organizzativo, di processo, tecnologico, di numero / tipologie di attività di trattamento
- Predisposizione e manutenzione del Registro indispensabile per avere il presidio dei dati trattati, dei soggetti, interni ed esterni, coinvolti nelle attività di trattamento, delle tecnologie / strumenti utilizzati per il trattamento

Warning

- Ogniqualvolta si effettua un nuovo trattamento di dati o se ne modifica uno preesistente, aggiornare il Registro delle attività di trattamento.

Adeguamento al GDPR

Valutazione di impatto sulla protezione dei dati personali

Principali riferimenti normativi

- Art. 35 del GDPR «*Valutazione d'impatto sulla protezione dei dati personali*»
- Art. 36 del GDPR «*Consultazione preventiva all'Autorità di Controllo*»

Principali punti d'attenzione

- A seguito di Risk Assessment, se il trattamento presenta un rischio elevato per i diritti e le libertà degli Interessati, prima di procedere al trattamento, si esegue obbligatoriamente la valutazione dell'impatto sulla protezione dei dati.
- La DPIA è uno strumento importante in termini di responsabilizzazione (accountability) in quanto aiuta il titolare non soltanto a rispettare le prescrizioni del GDPR, ma anche ad attestare di aver adottato misure idonee a garantire il rispetto di tali prescrizioni. In altri termini, la DPIA è una procedura che permette di valutare e dimostrare la conformità con le norme in materia di protezione dei dati personali. Vista la sua utilità, il Gruppo Art. 29 suggerisce di valutarne l'impiego per tutti i trattamenti, e non solo nei casi in cui il Regolamento la prescrive come obbligatoria

Warning

- Il Titolare del trattamento, prima di procedere al trattamento, consulta l'Autorità di Controllo, qualora la DPIA indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare stesso per attenuare il rischio.

Adeguamento al GDPR

Gestione del Data Breach

Principali riferimenti normativi

- Art. 33 del GDPR «*Notifica di una violazione dei dati personali all'autorità di controllo*»
- Art. 34 del GDPR «*Comunicazione di una violazione dei dati personali all'interessato*»

Principali punti d'attenzione

- Per «violazione dei dati personali» si intende la 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.
- Se il rischio / impatto della violazione per gli interessati è «Alto», notificazione della violazione al Garante della Privacy entro 72 ore dalla rilevazione. La violazione può essere notificata, in funzione del caso, agli interessati.
- Chiunque, all'interno dell'organizzazione, può rilevare il Data Breach

Warning

- Qualora si dovesse verificare un data breach, comunicare le informazioni relative alla violazione al FPP di Gruppo ed al DPO

Adeguamento al GDPR

Gestione del Data Breach

Violazione dei dati personali

Art. 4, n. 12: la 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

Notifica all'Autorità di controllo

Il Titolare del trattamento **notifica all'Autorità di controllo** la violazione: **senza ingiustificato ritardo e, ove, possibile, entro 72 ore** dal momento in cui è venuto a conoscenza della violazione

Comunicazione all'interessato

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento **comunica la violazione all'interessato** inserendo almeno le **informazioni** relative a:

- **nome e i dati di contatto del responsabile della protezione dei dati** o di altro punto di contatto;
- probabili **conseguenze della violazione dei dati personali**;
- **misure adottate** o di cui si propone l'adozione da parte del titolare del trattamento **per porre rimedio alla violazione**

Adeguamento al GDPR

Esempio di norme comportamentali da seguire nell'attività di trattamento

ID	Area tematica / Ambito	Raccomandazioni	Impatti correlati *(in caso di mancata osservanza)*		
			R	I	D
1	▪ **Gestione cartaceo**	▪ Evitare di tenere sulla scrivania / piani di lavoro, la documentazione non strettamente necessaria	X	X	X
2		▪ Si consiglia di riporre la documentazione cartacea negli appositi archivi cartacei, immediatamente dopo l'uso, assicurandosi di chiudere a chiave gli stessi, ove possibile	X	X	X
3	▪ **Gestione Posta Elettronica**	▪ Si raccomanda di utilizzare la posta elettronica dell'Ente esclusivamente per consentire lo svolgimento della propria attività lavorativa		X	
4	▪ **Utilizzo Internet**	▪ Si raccomanda di limitare l'accesso ad Internet evitando di accedere a siti non attinenti allo svolgimento delle mansioni assegnate	X	X	X
5	▪ **Credenziali di accesso** ***(Username e PSW per accesso a sistemi / applicativi)***	▪ Evitare di trascrivere le proprie credenziali di accesso su fogli di carta o di memorizzarle su supporti elettronici non protetti	X	X	
6		▪ Si raccomanda di non condividere / rivelare le proprie credenziali di accesso a PC, Sistemi, mail con / ad altri utenti / Terzi	X	X	
7	▪ **Condivisione Informazioni**	▪ Astenersi dal comunicare le informazioni relative alla propria attività lavorativa a terzi	X		
8	▪ **Mail Sospette** ***(es. Phishing)***	▪ Evitare di aprire e-mail sospette. Qualora dovessero essere aperte, evitare di cliccare sul link ivi inserito, comunicando immediatamente la presenza della mail a fornitori IT e colleghi	X	X	X
9	▪ **Documenti di lavoro a casa**	▪ Si raccomanda di non portare fuori dai luoghi di lavoro i documenti	X		
10	▪ **Dispositivi mobili**	▪ Evitare di archiviare documenti / informazioni su supporti rimovibili, se non adeguatamente protetti	X	X	

Legenda R Riservatezza del dato I Integrità del dato D Disponibilità del dato

Adeguamento al GDPR

Sommario delle principali novità

1. Perimetro

La riforma coinvolge tutti gli Stati UE e chiunque tratti dati di cittadini europei.

2. Responsabilità

Viene disciplinato in modo più dettagliato il ruolo di responsabile del Trattamento.

3. Informazioni chiare

Viene rafforzato l'obbligo di fornire informative semplici e chiare al fine di rafforzare il controllo degli interessati.

4. Diritto all'oblio

Diritto dell'interessato di ottenere dal titolare del trattamento la cancellazione dei dati personali al ricorrere di determinate specifiche ipotesi.

5. Portabilità dei dati

Diritto alla portabilità del dato che permette all'interessato di ricevere i propri dati su un formato strutturato e leggibile e/o di farli trasmettere da un titolare all'altro.

6. Privacy by design & by default

Il titolare deve implementare misure idonee a proteggere i dati sin dal momento di progettazione del trattamento, garantendone il trattamento dei dati necessari al perseguimento delle finalità per cui sono raccolti.

7. Data Breach Notification

Determinate violazioni di dati devono essere segnalate sia al Garante che agli interessati senza ritardo e, in alcuni casi, entro 72 ore dalla violazione.

8. Data Protection Impact Assessment

Obbligo per ciascun Titolare di svolgere, e documentare, una autovalutazione del rischio derivante dai trattamenti effettuati e, sulla base degli esiti delle analisi, di effettuare una consultazione preventiva

9. Responsabile della Protezione dei dati

Responsabile della Protezione dei dati (RPD) addetto a: sorvegliare l'osservanza delle disposizioni privacy, fornire consulenza e pareri, fungere da contatto con il Garante o gli interessati.

10. Registri del trattamento

Obbligo di conservare, anche in formato elettronico, un registro dei trattamenti effettuati, contenente alcuni specifici dettagli.

11. Sanzioni

Sino ad un massimo di € 20.000.000 o al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

A business of Marsh McLennan