



GDPR

General Data Protection Regulation

D.Lgs. 101/2018 – Decreto Attuativo che integra e modifica 196/2003



1



OBBLIGHI INTRODOTTI DAL REGOLAMENTO UE 679/2016

- **Rispettare i diritti degli interessati:** ogni trattamento deve fondarsi sul rispetto dei principi indicati dal Regolamento (artt. 5-6) e garantire agli interessati tutti i diritti previsti (artt. 13-22)
- **Redigere un Registro delle Attività di Trattamento (art. 30):** strumento fondamentale per disporre di un quadro aggiornato dei trattamenti in essere. I contenuti minimi sono indicati all'art. 30 del Regolamento. Deve avere forma scritta, anche elettronica, e va esibito su richiesta al Garante.
- **Garantire la sicurezza dei dati:** Il titolare e il responsabile del trattamento sono obbligati ad adottare misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio del trattamento (con l'obiettivo di evitare distruzione accidentale o illecita, perdita, modifica, rivelazione, accesso non autorizzato)

3



DEFINIZIONI

DATI PERSONALI qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente	CATEGORIE PARTICOLARI DI DATI PERSONALI (Art. 9) dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici o biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona
---	--

2



OBBLIGHI INTRODOTTI DAL REGOLAMENTO UE 679/2016

- **Effettuare una Valutazione del Rischio (art. 32):** ai titolari spetta il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, anche attraverso un apposito processo di valutazione che tenga conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) necessarie per mitigare tali rischi, eventualmente consultando il Garante alla luce di questa valutazione.
- **Effettuare una Valutazione d'Impatto:** nei casi previsti dall'art. 35 o se dalla Valutazione del Rischio risulta esserci un rischio residuale elevato.
- **Nominare un Responsabile della Protezione dei Dati:** nei casi previsti dall'art. 37.

4

PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI PERSONALI (Art. 5)



- I dati personali sono:
 1. Trattati in modo LECITO, CORRETTO e TRASPARENTE;
 2. Raccolti per FINALITÀ DETERMINATE, ESPLICITE E LEGITTIME;
 3. ADEGUATI, PERTINENTI E LIMITATI a quanto necessario per le finalità per cui sono trattati;
 4. ESATTI E SE NECESSARIO AGGIORNATI;
 5. CONSERVATI in una forma che consenta l'identificazione degli interessati PER UN ARCO DI TEMPO NON SUPERIORE AL CONSEGUIMENTO DELLE FINALITÀ;
 6. TRATTATI IN MANIERA DA GARANTIRE UN'ADEGUATA SICUREZZA dei dati personali.

5

CONSENSO (Art. 7)



- **ESPLICITO**: per le categorie particolari di dati personali;
- **INFORMATO**
- **PROVATO**: non è necessaria la forma scritta ma serve a dimostrare in maniera univoca l'espressione del consenso da parte dell'interessato;
- **SPECIFICO**: serve un consenso esplicito per ogni finalità per cui verranno trattati i dati.

CONSENSO MINORI DI 14 ANNI: rilasciato da chi esercita la responsabilità genitoriale (entrambi i genitori).

NB: l'interessato in qualsiasi momento ha il DIRITTO DI REVOCARE IL CONSENSO

7

PRINCIPI DI LICEITÀ (Art. 6)



il trattamento è lecito se ricorre almeno una delle seguenti condizioni:

1. Consenso espresso dall'interessato;
2. Esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
3. Adempimento ad un obbligo legale al quale è soggetto il Titolare del Trattamento;
4. Necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
5. Necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del Trattamento.

6

CONSENSO (Art. 7)



Art. 13 – comma 3:

«Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente»

IL CONSENSO DEVE ESSERE SPECIFICO PER UNA FINALITÀ

8

INFORMATIVA (Art. 13)



Contenuti dell'informativa:

- Identità e dati di contatto del Titolare del Trattamento;
- Identità e dati di contatto del Responsabile del Trattamento;
- Le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- Interessi legittimi perseguiti dal Titolare del Trattamento qualora il trattamento si basi sull'art. 6
- Eventuali destinatari o categorie di destinatari dei dati;
- Ove applicabile l'intenzione del Titolare del Trattamento di trasferire i dati personali a un paese terzo.

9

DIRITTI DEGLI INTERESSATI:



- Accesso (Art. 15);
- Rettifica (Art. 16);
- Cancellazione (Art. 17);
- Limitazione del trattamento (Art. 18);
- Opposizione (Art. 20).

11

INFORMATIVA (Art. 13)

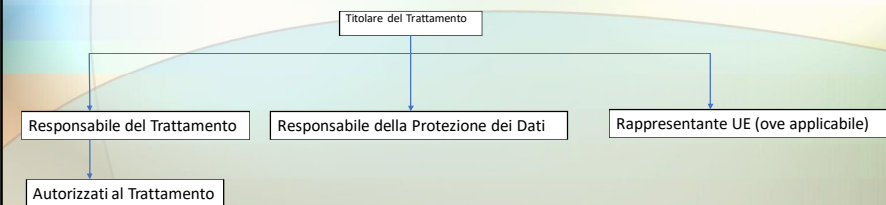


Contenuti dell'informativa:

- Identità e dati di contatto del Responsabile della Protezione dei Dati (DPO/RPD);
- Periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo;
- I diritti dell'interessato (rettifica, cancellazione, limitazione, ecc.);
- Il diritto di proporre reclamo a un'autorità di controllo;
- Se la comunicazione dei dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
- L'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'art. 22 e se presente, le informazioni sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

10

ORGANIGRAMMA



12

TITOLARE DEL TRATTAMENTO (Art. 24)



- Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento 679/2016. Aggiornare e riesaminare le misure qualora necessario.
- Nomina, tramite contratto o altro atto giuridico, il Responsabile del Trattamento.

13

RESPONSABILE DELLA PROTEZIONE DEI DATI (Art.37)



Designazione obbligatoria ogniqualvolta:

- Il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico;
- Le attività principali del titolare del trattamento consistono in attività che, per loro natura, richiedono il monitoraggio sistematico e regolare degli interessati;
- Le attività principali del titolare del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali.

15

RESPONSABILE DEL TRATTAMENTO (Art. 28)



Obblighi:

- Trattare i dati personali solo su istruzione documentata e scritta del titolare del trattamento;
- Garantire che le persone autorizzate al trattamento si siano impegnate alla riservatezza o abbiano un obbligo legale di riservatezza;
- Adottare tutte le misure richieste ai sensi dell'art. 32;
- Assistere il titolare del trattamento con misure tecniche e organizzative adeguate;
- Assistere il titolare del trattamento nel rispettare gli obblighi;
- Cancellare o restituire i dati su scelta del titolare del trattamento;
- Mettere a disposizione del titolare tutte le informazioni necessarie a dimostrare il rispetto degli obblighi.

14

RESPONSABILE DELLA PROTEZIONE DEI DATI (Art.37)



Compiti del RPD:

- Informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti;
- Sorvegliare l'osservanza del Regolamento;
- Fornire, se richiesto, pareri in merito alla valutazione d'impatto e sorvegliarne lo svolgimento;
- Cooperare con le autorità;
- Fungere da punto di contatto per l'autorità di controllo.

16

REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO (Art. 30)



Contenuti:

- Processo/ macro attività di trattamento;
- Finalità del trattamento;
- Descrizione delle categorie di dati personali trattati e degli interessati;
- Categorie dei destinatari a cui saranno comunicati i dati;
- Eventuali trasferimenti di dati a paesi extra UE;
- Termini ultimi per la cancellazione dei dati;
- Descrizione delle misure di sicurezza tecniche ed operative.

17

VALUTAZIONE DEL RISCHIO (Art. 32)



La valutazione del rischio è data dalla combinazione di due coefficienti:

- **probabilità** di accadimento della minaccia rilevata (la probabilità è legata anche all'esistenza o meno di strumenti di controllo/regole atti a prevenire il verificarsi della minaccia rilevata) ;
- **danno**, inteso come possibile applicazione alla società delle misure sanzionatorie oppure danni materiali derivanti dal verificarsi dell'evento considerato a rischio.

19

VALUTAZIONE DEL RISCHIO (Art. 32)



Il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato, tra le altre:

- La pseudonimizzazione e la cifratura dei dati personali;
- Capacità di assicurare su base permanente la riservatezza, l'integrità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- Capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- Procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative.

18

VALUTAZIONE DEL RISCHIO (Art. 32)



PROBABILITÀ	ALTA (3)	3	6	9
	MEDIA (2)	2	4	6
	BASSA (1)	1	2	3
		MINIMO (1)	MEDIO (2)	SIGNIFICATIVO (3)
		DANNO		

Indice di rischio	Livello di Rischio
6 + 9	Significativo (Azione urgente)
2 + 4	Medio (Azione richiesta)
1	Minimo (Monitor)

20

VALUTAZIONE DI IMPATTO (Art. 35)



Obbligatoria (in presenza di almeno due di questi criteri)

- Trattamenti valutativi o di scoring, compresa la profilazione;
- Decisioni automatizzate che producono significativi effetti giuridici;
- Monitoraggio sistematico (es. videosorveglianza);
- Trattamento di dati sensibili, giudiziari o di natura estremamente personale;
- Trattamenti di dati personali su larga scala;
- Trattamenti svolti secondo modalità che esulino dal consenso iniziale;
- Dati relativi a soggetti vulnerabili;
- Utilizzi innovativi o applicazioni di nuove soluzioni tecnologiche (es. riconoscimento facciale);
- Trattamenti che potrebbero impedire agli interessati di esercitare un diritto.

Non obbligatoria

- Non presente rischio elevato per diritti e libertà delle persone fisiche;
- Sono già stati sottoposti a verifica da parte di un'Autorità di controllo;
- Sono compresi nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere con la DPIA;
- Fanno riferimento a norme e regolamenti, per la cui definizione è stata condotta una DPIA.

21

RIEPILOGO PRINCIPALI NOVITÀ



SCOMPANIONO	SI INTRODUCONO
Obbligo di notificazione di verifica preliminare al Garante	Obbligo tenuta del registro dei trattamenti (art. 30 GDPR)
Obbligo di consenso in forma scritta dei dati sensibili	Nessuna misura introdotta, ma resta lecito il consenso in forma scritta per dimostrare che il l'interessato ha prestato il consenso al Titolare
Misure minime ed idonee (rif. "Allegato B" D.Lgs. 196/2003)	Art. 32 Reg. Generale 679/2016 "Misure adeguate per la tutela delle banche dati"
//	Obbligo generalizzato di notifica al Garante per le violazioni della sicurezza dei dati (Notifica violazioni)
//	Obbligo valutazione di impatto sulla protezione dei dati, da effettuarsi in caso di rischio "alto" (se il rischio residuo rimane alto occorre procedere alla consultazione preventiva del Garante)
//	Diritto alla portabilità
//	Diritto di aggiornamento, rettifica o cancellazione
Diritto di blocco	Diritto alla limitazione (di maggiore interesse per gli informatici)
//	Diritto all'opposizione al trattamento (anche senza lecito motivo)
//	Obbligo di designare un Responsabile della Protezione dei Dati nei casi di cui all'art. 37 del GDPR

23

CONSULTAZIONE PREVENTIVA (Art. 36)



Se nonostante tutte le misure di sicurezza adottate a seguito della Valutazione di impatto, il rischio rimane alto, si deve procedere con la consultazione preventiva al Garante (parere).

In tal caso, il titolare del trattamento comunica all'autorità di controllo:

- Responsabilità delle figure del sistema privacy (titolare del trattamento, responsabile del trattamento)
- Finalità e mezzi del trattamento previsto
- Misure e garanzie previste per proteggere i diritti e le libertà degli interessati
- I dati di contatto del RPD
- La valutazione di impatto
- Ogni altra informazione richiesta dall'autorità di controllo

22

SANZIONI (Art. 83)



Il GDPR ha previsto **rilevanti sanzioni di natura amministrativa** in caso di violazioni della normativa sulla protezione dei dati personali.

L'art. 83 del GDPR distingue **due gruppi di sanzioni amministrative**:

- 1) violazioni cosiddette di minore gravità
- 2) violazioni più pesanti



24

SANZIONI (Art. 83)



VIOLAZIONI DI MINORE GRAVITÀ, per le quali sono previste le sanzioni amministrative pecuniarie di importi fino a 10 milioni di euro o, per le imprese 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:

- *il titolare ed il responsabile del trattamento*
- *l'organismo di certificazione, Accredia*
- *l'organismo di controllo dei codici di condotta (art. 41 GDPR)*

VIOLAZIONI PIÙ PESANTI in considerazione della maggiore gravità delle fattispecie a cui sono ricondotte, ammontano fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, e riguardano nello specifico le seguenti violazioni:

- *principi di base del trattamento*
- *condizioni relative al consenso*
- *diritti degli interessati*
- *trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale*
- *inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo (ovvero il Garante Privacy)*