



**EMMEC**  
Legal & Privacy

# La figura del DPO

Artt. 37, 38, 39 Regolamento (UE) 679/2016

Pisa, 26 ottobre 2021

**Avv. Filippo Castagna**

[info@studioemmec.it](mailto:info@studioemmec.it)

## Chi è il DPO: Data Protection Officer

Il Data Protection Officer (di seguito DPO) è una figura introdotta dal Regolamento generale sulla protezione dei dati 2016/679.

Il DPO, figura storicamente già presente in alcune legislazioni europee, è un professionista che deve avere un ruolo aziendale (sia esso soggetto interno o esterno) con competenze giuridiche, informatiche, di risk management e di analisi dei processi. La sua responsabilità principale è quella di:

- osservare, valutare e organizzare la gestione del trattamento di dati personali all'interno di un'azienda (sia essa pubblica che privata),
- affinché questi siano trattati nel rispetto delle normative privacy europee e nazionali.

# LA NOMINA DEL DPO

Il DPO è designato dal titolare del trattamento e/o dal responsabile del trattamento ognqualvolta:

- a) Siano un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
- b) le loro attività principali consistano in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure
- c) le loro attività principali consistano in trattamenti, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

# ....in particolare circa la nomina del DPO

- Le **attività principali** del titolare o del responsabile [...] richiedono il **monitoraggio regolare e sistematico su larga scala** degli interessati o trattamento su **larga scala di particolari categorie di dati** (artt. 9 e 10 GDPR);
- **Attività principale**: oltre l'ovvio significato non si possono escludere quelle attività che costituiscono **componenti inscindibili** dell'attività principale. Es: *clinica privata* (servizi forniti e dati sanitari trattati);
- **Larga scala**: concorrono a determinare il criterio: il numero dei soggetti interessati al trattamento; il volume dei dati trattati; la durata; la portata geografica del trattamento; (Es: banche e assicurazione; Fornitori di servizi telefonici o telematici, Cliniche private e Case di cura);
- **Monitoraggio regolare e sistematico**: criteri necessariamente cumulativi e non alternativi. Es: programmi di fidelizzazione, monitoraggio dati sulla salute (*wearables devices*), etc.

# **La designazione del responsabile della protezione dei dati (DPO) - art. 37**

Il responsabile della protezione dei dati è designato in funzione delle **qualità professionali**, in particolare della **conoscenza specialistica della normativa e delle prassi in materia** di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39.

Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi.

Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo.

# Requisiti e formalità della nomina

- Conoscenza non semplice ma specialistica della normativa e della prassi;
- Differenza tra DPO e Responsabile del trattamento dei dati;
- Nomina mediante contratto di servizi se DPO è soggetto esterno (ex art. 37, par. 6);
- Comunicazione dei dati del DPO all'autorità di controllo (Garante Privacy);
- Indicazione sulle informative predisposte dal titolare del trattamento.

# FOCUS PROCEDURA DI NOMINA

- Trattasi di una procedura molto semplice, da effettuare secondo le istruzioni presenti sul sito web dell'Autorità Garante per la protezione dei dati personali;
- La comunicazione deve essere fatta dal legale rappresentante del titolare/responsabile del trattamento dei dati, o da un suo delegato che dovrà compilare un modulo apposito;
- Bisogna poi utilizzare l'**Identificativo Provvisorio della Comunicazione e del PIN inviato tramite mail dal Garante**;
- è necessario disporre di un **dispositivo di firma digitale** con cui sottoscrivere in formato CAdES il file contenente i dati forniti durante la compilazione del modulo iniziale.

# FOCUS CASO PRATICO

## L’Ospedale privato nomina il DPO

(Provvedimento Garante Privacy n. 55 del 7 marzo 2019)

Norme di riferimento: art. 37 Regolamento

Si ritiene che anche il trattamento dei dati relativi a pazienti svolto da un ospedale privato, da una casa di cura o da una residenza sanitaria assistenziale (RSA) possa rientrare, in linea generale, nel concetto di larga scala. (Linee guida sui Responsabili della protezione dei dati, WP243, adottate il 13 dicembre 2016, versione emendata e adottata in data 5 aprile 2017, punto 2.1.3, doc. web n. 612048, fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018, cfr. Endorsement n. 1/2018).

# Posizione del responsabile della protezione dei dati – art. 38

1. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia **tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.**
2. Il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 **fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali** e ai trattamenti e per mantenere la propria conoscenza specialistica.
3. Il titolare del trattamento e il responsabile del trattamento si assicurano che **il responsabile della protezione dei dati non riceva alcuna istruzione** per quanto riguarda l'esecuzione di tali compiti.
- 4 Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.

# Il coinvolgimento del DPO

- Coinvolgimento del DPO in tutte le questioni riguardanti la protezione dei dati personali
- Consultazione del DPO per quanto riguarda la valutazione di impatto del trattamento sui dati personali, sin dall'inizio del conferimento di incarico;
- Destinazione di risorse al DPO;
- Prescrizioni del WP29:
  - Partecipazione del DPO alle riunioni del management;
  - Presenza necessaria ognqualvolta si debbano assumere decisioni che impattano sulla protezione dei dati;
  - Il parere del DPO deve ricevere attenzione da parte del Titolare o del Responsabile del trattamento; necessità di documentare l'eventuale dissenso dal parere del DPO;

# QUALI SONO I COMPITI DEL DPO?

1. Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:

- a) **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 dalla normativa in materia;
- b) **sorvegliare l'osservanza della normativa in materia;**
- c) **fornire, se richiesto, un parere in merito alla valutazione d'impatto** sulla protezione dei dati e sorveglierne lo svolgimento ai sensi dell'articolo 35;
- d) **cooperare con l'autorità di controllo;** e
- e) **fungere da punto di contatto per l'autorità di controllo** per questioni connesse al trattamento, tra cui la consultazione preventiva ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

2. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

# I compiti del DPO

- L'elencazione di cui all'art. 39 GDPR non è tassativa (...almeno i compiti...)
- Assistenza al titolare nella gestione dei data breach;
- Tenuta del registro dei trattamenti;
- Adozione di audit interni al fine di monitorare l'attività di Titolare e del Responsabile, suggerendo iniziative anche di carattere tecnologico al fine di adeguare la struttura, sempre con riferimento alle capacità patrimoniali del soggetto tenuto alla loro adozione.
- Nell'esecuzione dei propri compiti il DPO non ha responsabilità verso terzi né è destinatario di sanzioni amministrative (differenza con Titolare e Responsabile del trattamento);

# QUANDO IL DPO È RESPONSABILE?

La responsabilità in capo al DPO è di natura contrattuale, pertanto, egli può ritenersi responsabile nei confronti del Titolare del trattamento dei dati (che lo nomina) allorquando venga meno ai propri doveri.

Il DPO non ha tuttavia responsabilità nei confronti dei soggetti terzi che si ritengano lesi da condotte tenute in violazione del Regolamento tenute dal titolare.

Allo stesso modo sempre il DPO, non sarà responsabile allorquando il Titolare abbia disatteso le indicazioni fornite in materia di trattamento.



EMMEC  
Legal & Privacy

# **CONSULENZA: LA CORRETTA INDIVIDUAZIONE DEI SOGGETTI COINVOLTI**

## FOCUS

# QUANDO I CONSULENTI DEL LAVORO SONO TITOLARI DEL TRATTAMENTO

Doc. web. n. 9080970

I consulenti del lavoro sono titolari quando trattano in piena autonomia indipendenza i dati dei propri dipendenti oppure dei propri clienti quando siano persone fisiche come esempio liberi professionisti determinando puntualmente le finalità e mezzi del trattamento.

Sulla base del principio affermato i consulenti del lavoro devo compilare il registro dei trattamenti di intitolare a fornire un'informativa in cui indicano la loro qualifica.

# FOCUS

## QUANDO I CONSULENTI DEL LAVORO SONO RESPONSABILI DEL TRATTAMENTO

Doc. web. n. 9080970

I consulenti del lavoro sono responsabili del trattamento quando trattano i dati dei dipendenti dei loro clienti sulla base dell'incarico ricevuto, il quale contiene anche le istruzioni sui trattamenti da effettuare.

Sulla base del principio affermato, tra committente consulente del lavoro deve essere sottoscritto il contratto di responsabile del trattamento quando, ad esempio, i consulenti curano per conto più datori di lavoro la predisposizione delle buste paga, le pratiche relative all'assunzione a fine rapporto o quelle previdenziali e assistenziali, trattando una pluralità di dati personali, anche sensibili, dei lavoratori.

# **FOCUS**

## **IL GESTORE DEL SITO INTERNET**

Doc. web. n. 9207876

Il titolare del trattamento che affida il suo sito web a una società di servizi informatici deve nominare quest'ultima quale responsabile del trattamento.

Commette un illecito il titolare che comunica i dati dei suoi clienti a una società incaricata di gestire il sito web, senza che la stessa sia stata nominata responsabile del trattamento.

Stessa cosa per servizi di web hosting, caselle email e spazi sul cloud.

## FOCUS

# LA SOCIETÀ ASSICURATRICE AGGIUDICATARIA DI UN APPALTO È AUTONOMO TITOLARE RISPETTO ALL'ENTE COMMITTENTE

Doc. web. n. 9169688

Quando un ente pubblico appalta il servizio assicurativo, la società assicuratrice, futura aggiudicataria del servizio di copertura assicurativa, agisce in qualità di autonomo titolare del trattamento e non quale responsabile.

Ai fini delle qualificazione quale titolare o responsabile, non rileva a tal fine la modalità con la quale l'ente aggiudicante effettua la scelta o la selezione del soggetto che fornirà il servizio, a prescindere dalla qualificazione fornita astrattamente da quest'ultimo.

Nel caso di specie, la società aggiudicatrice agisce in qualità di autonomo titolare in quanto non pone in essere un trattamento di dati per conto dell'ente aggiudicante, circostanza che la priverebbe dell'autonomia necessaria ad una corretta valutazione e liquidazione del danno.

## Misure di sicurezza

Sia il titolare del trattamento che il responsabile, sono tenuti ad attuare le **misure tecniche ed organizzative** tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

Si tratta di specifici requisiti previsti dal GDPR, che indica alcune misure di sicurezza utili per ridurre i rischi del trattamento, quali la pseudonimizzazione e la cifratura dei dati personali, la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Il responsabile può dimostrare le garanzie sufficienti anche attraverso l'adesione a **codici deontologici** ovvero a **schemi di certificazione**.

# Misure di sicurezza tecniche

- Cifratura dei dati;
- Pseudonimizzazione;
- Antivirus/Firewall;

# Misure di sicurezza organizzative

- Nomina DPO;
- Formazione dipendenti;
- Modello Organizzativo Privacy (MOP)

# FOCUS

## LA DESIGNAZIONE DEGLI AUTORIZZATI

**Provvedimento n. 111 del 6 maggio 2019, doc. web. n. 9164171**

Norme interessate art. 29 GDPR - art. 2 quaterdecies Codice Privacy

Il titolare del trattamento deve designare quale autorizzati i dipendenti adibiti alla gestione delle proprie attività.

In mancanza di una designazione, può essere contestata la violazione dell'obbligo di adottare misure organizzative concernenti la misura sicurezza ai trattamenti.

Sulla base del principio affermato il titolare del trattamento deve autorizzare e formare ogni singolo dipendente.

Dovrà inoltre impartire istruzioni in vari soggetti autorizzati che individuino puntualmente l'ambito del trattamento consentito, indicando in particolare le modalità con cui gli autorizzati dovranno trattare, gestire conservare i dati acquisiti.

## DATA PROTECTION E CYBER SECURITY

Right to be let alone - right to privacy

right to data protection

Cybersecurity

Spesso vi è sovrapposizione fra questi concetti perché nell'attuale contesto informatico la protezione dei dati personali assume una dimensione ormai quasi esclusivamente tecnologica.

*Cybersecurity quell'insieme di tecnologie, programmi, processi e tecniche concepiti e messi in atto per proteggere dispositivi, dati e reti informatiche.*

## DATA PROTECTION E CYBER SECURITY

Cybersecurity: sicurezza del contenitore informatico.

Data Protection: sicurezza delle informazioni contenute all'interno.

## RISK ASSESSMENT

Un "rischio" è uno scenario che descrive un evento e le sue conseguenze, stimate in termini di gravità e verosimiglianza.

La "valutazione del rischio" può essere definita come l'attività coordinata per dirigere e controllare un'organizzazione in relazione al rischio.

Elementi da considerare nella valutazione del rischio:  
origine, natura, gravità, probabilità, impatto sui diritti e sulle libertà delle persone.

# RISK ASSESSMENT

La sicurezza del trattamento e gli effetti generali dello stesso.

Errori comuni:

Non bisogna confondere la gestione dei rischi con il tema delle misure di sicurezza;

Il rischio non si riferisce al titolare ma al soggetto interessato.

# RISK ASSESSMENT

**DISPONIBILITÀ** -*distruzione - indisponibilità - perdita*

**INTEGRITÀ** -*alterazione*

**RISERVATEZZA** -*divulgazione - accesso*

Danno per la reputazione  
Discriminazione  
Furto d'identità  
Perdite finanziarie  
Danni fisici o psicologici  
Perdita di controllo dei dati  
Altri svantaggi economici o sociali  
Impossibilità di esercitare diritti, servizi o opportunità

# La valutazione d'impatto (DPIA)

**Quando un tipo di trattamento**, allorché **prevede in particolare l'uso di nuove tecnologie**, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, **può presentare un rischio elevato per i diritti e le libertà delle persone fisiche**, il titolare del trattamento **effettua**, prima di procedere al trattamento, **una valutazione dell'impatto** dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:

- 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 di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;
- c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

## RISCHIO=IMPATTO x PROBABILITÀ

MOLTO ALTO	5	10	15	20	25
ALTO	4	8	12	16	20
MEDIO	3	6	9	12	15
BASSO	2	4	6	8	10
MOLTO BASSO	1	2	3	4	5
	MOLTO BASSO	BASSO	MEDIO	ALTO	MOLTO ALTO
			<u>PROBABILITÀ</u>		

# La valutazione d'impatto (DPIA)

1. Trattamenti valutativi o di *scoring* su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad *"aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato"*.
2. Trattamenti automatizzati finalizzati ad assumere decisioni che producono *"effetti giuridici"* oppure che incidono *"in modo analogo significativamente"* sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. *screening* dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi).
3. Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi *web*, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di *budget*, di *upgrade* tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.

# La valutazione d'impatto (DPIA)

4. Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).
5. Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali deriva la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).
6. Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).
7. Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi *wearable*; tracciamenti di prossimità come ad es. il *wi-fi tracking*) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01 .
8. Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.
9. Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. *mobile payment*).

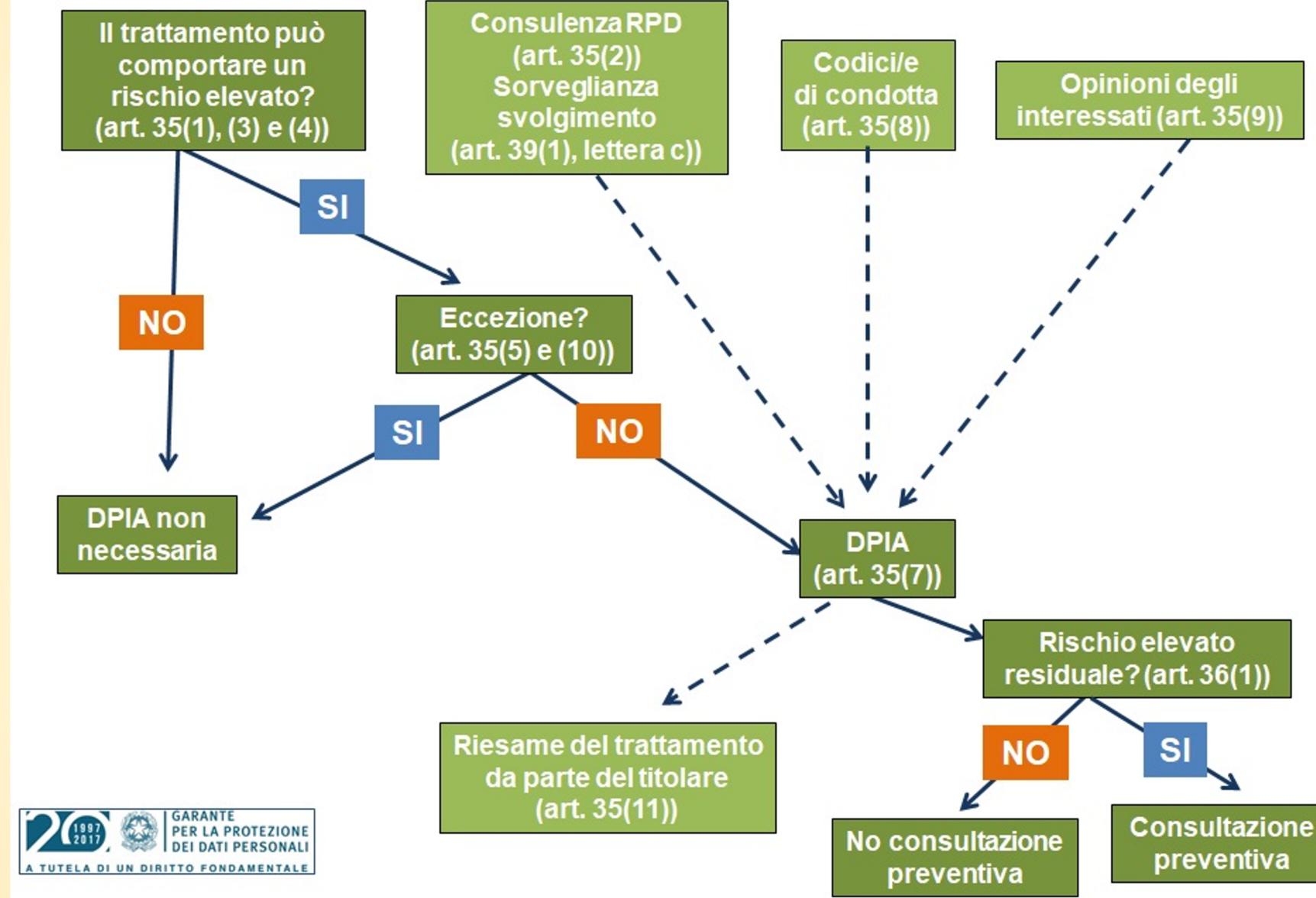
# La valutazione d'impatto (DPIA)

10. Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.
11. Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.
12. Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

# Valutazione di impatto sulla protezione dei dati (DPIA). Quando effettuarla?



EMMEC  
Legal & Privacy





EMMEC  
Legal & Privacy

# FOCUS IL SOFTWARE DEL CNIL

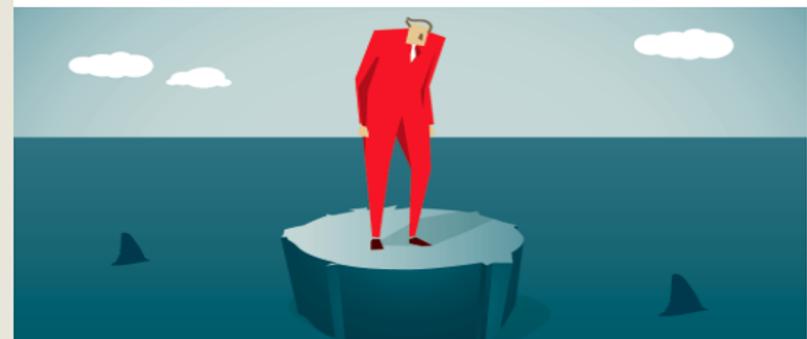
**CNIL.**  
*To protect personal data, support innovation, preserve individual liberties*

MY COMPLIANCE TOOLS | DATA PROTECTION | TOPICS | THE CNIL | Q |

> GDPR toolkit > Privacy Impact assessment (PIA)

## Privacy Impact Assessment (PIA)

*Where a processing is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall carry out a privacy impact assessment.*



**DPIA guidelines**

WP29 has published guidelines on Data Protection Impact Assessment in order to propose a joint explanation and interpretation of Art.35 of GDPR.

[> Guidelines](#)

**PIA Software**

Available in its beta version, the software helps data controller to carry out PIA and demonstrate compliance to GDPR.

[> Software](#)

**PIA Guides**

A set of documents (PIA methodology, knowledge base and case studies) aiming to assess the privacy risks of a processing

# I DIRITTI DELL'INTERESSATO

## (Artt. 15-22 GDPR)

In tema di diritti dell'interessato il Legislatore Comunitario ha rielaborato i principi che reggevano la vecchia disciplina in tema di privacy, riformulandone nella lunga elencazione (che va dall'art. 15 al 22 del GDPR) nuove prerogative riconosciute agli interessati al trattamento, tenendo in considerazione l'attuale sviluppo delle nuove tecnologie che potenzialmente possono determinare nuovi pericoli e rischi per i diritti e le libertà degli stessi.

## IL DIRITTO DI ACCESSO - art. 15 GDPR

### INFORMAZIONI DA FORNIRE ALL'INTERESSATO

- 1) finalità del trattamento;
- 2) categorie di dati personali in questione;
- 3) destinatari o le categorie di destinatari a cui i dati personali sono o saranno comunicati;
- 4) il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare questo periodo);
- 5) l'esistenza di un processo decisionale automatizzato, compresa l'eventuale attività di profilazione.

## IL DIRITTO DI RETTIFICA - art. 16 GDPR

Diritto di ottenere la rettifica dei dati che lo riguardano ed, eventualmente, la loro integrazione.

## FOCUS

# COME GARANTIRE I DIRITTI DELL'INTERESSATO

L'esercizio dei diritti dell'interessato è subordinato alla sua identificazione.

Il titolare del trattamento deve fornire, entro i termini previsti, un adeguato riscontro agli interessati che esercitino i diritti previsti dagli articoli 15 - 22 Regolamento. Sulla base del principio affermato, se il titolare non risponde nei termini previsti dall'art. 12 del Regolamento (*al più tardi entro un mese dal ricevimento della richiesta stessa, salvo proroga giustificata*), si rende applicabile la sanzione di cui all'art. 83, par. 5 lett. b) del medesimo Regolamento. tale sanzione prevede l'applicazione di una sanzione fino ad un massimo di euro 20.000.000 o o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.



**EMMEC**  
Legal & Privacy

# GRAZIE PER L'ATTENZIONE

[info@studioemmec.it](mailto:info@studioemmec.it)  
[filippo@studioemmec.it](mailto:filippo@studioemmec.it)  
[avvfilippocastagna@gmail.com](mailto:avvfilippocastagna@gmail.com)