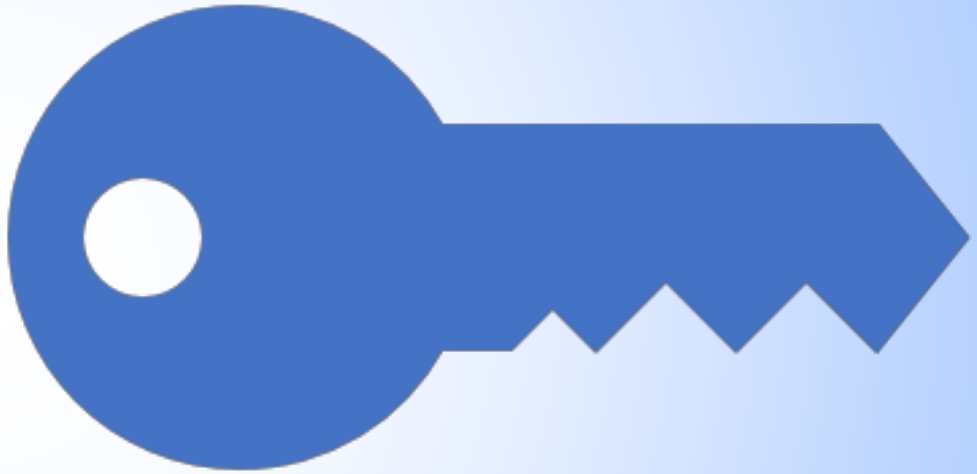
PRIVACY 4.R:

Regolamento
Ruoli
Rischi
Responsabilità



Roma, 18 Aprile 2019

Studio Legale De Vita

PRIVACY 4.R

SESSIONE 1

GDPR:
UNA NUOVA VISIONE PER LA TUTELA DEI DATI PERSONALI

PROF. AVV. ROBERTO DE VITA

STUDIO LEGALE DE VITA

General Data Protection Regulation (GDPR) Reg. (UE) 2016/679

25.05.2016

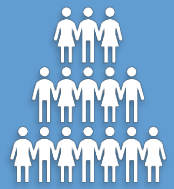
ENTRA IN VIGORE IL GDPR

25.05.2018

IL GDPR È APPLICABILE

IN TUTTI GLI STATI UE

General Data Protection Regulation (GDPR) Reg. (UE) 2016/679



Nuova definizione di «dato personale»

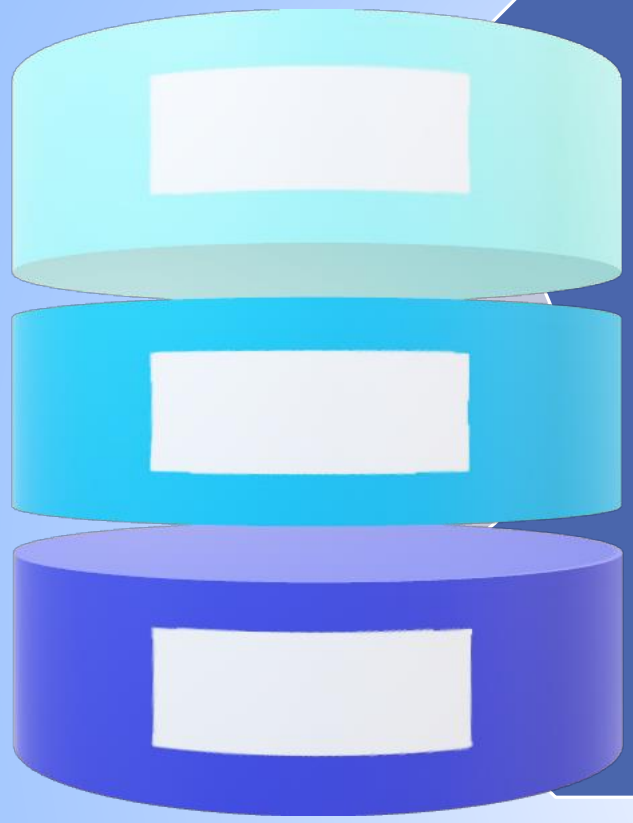
Principio di «Accountability»

Risk Based Approach: Privacy by design & Privacy by default

Art. 4 GDPR – Definizioni
DATO PERSONALE

Qualsiasi informazione riguardante una **persona fisica** identificata o identificabile («**interessato**»);

Si considera identificabile la persona che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il **nome**, un **numero di identificazione**, un **identificativo online** o a uno o più **elementi caratteristici** della sua identità fisica, fisiologica, genetica, economica, culturale o sociale.



Qualsiasi **operazione o insieme di operazioni**, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la **raccolta**, la **registrazione**, l'**organizzazione**, la **strutturazione**, la **conservazione**, l'**adattamento** o la **modifica**, l'**estrazione**, la **consultazione**, l'**uso**, la **comunicazione mediante trasmissione**, **diffusione** o qualsiasi altra forma di **messa a disposizione**, il **raffronto** o l'**interconnessione**, la **limitazione**, la **cancellazione** o la **distruzione**.

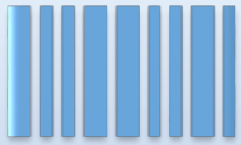
Art. 4 GDPR – Definizioni
TRATTAMENTO

Art. 4 GDPR – Definizioni
PROFILAZIONE

Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per **valutare determinati aspetti personali** relativi a 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.

Art. 4 GDPR – Definizioni

DATI BIOMETRICI E RELATIVI ALLA SALUTE



Dati biometrici – i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici

Dati relativi alla salute – i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute

TRATTAMENTO

PRINCIPI GENERALI (art. 5)

Liceità – Correttezza – Trasparenza

Limitazione della finalità

Minimizzazione dei dati e limitazione della conservazione

Esattezza

Integrità e riservatezza

Responsabilizzazione («Accountability»)

LICEITÀ DEL TRATTAMENTO (art. 6)

Il trattamento è lecito solo se ricorre una delle seguenti condizioni:

L'interessato ha espresso il consenso

Il trattamento è **necessario all'esecuzione di un contratto di cui l'interessato è parte**

Il trattamento è necessario **per adempiere un obbligo legale** al quale è soggetto il titolare del trattamento

Il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di altra persona fisica

Il trattamento è **necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri** di cui è investito il titolare

Il trattamento è necessario per il perseguimento del legittimo interesse del titolare a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato

LICEITÀ DEL TRATTAMENTO (art. 6)

CONSENSO

BASE GIURIDICA
(DIRITTO DELL'UE O DELLO STATO MEMBRO)

TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI (art. 9)

1) È **vietato trattare** dati personali che rivelino l'originale razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'**appartenenza sindacale**, nonché trattare 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.

TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI (art. 9)

2) Il paragrafo 1 non si applica se:

a) L'interessato ha prestato il proprio **consenso esplicito**

b) Il trattamento è necessario **per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale**, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri

c) […]

d) Il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, **da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità** politiche, filosofiche, religiose o **sindacali**, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato

Autorizzazione Generale n. 3/2016
Garante per la Protezione dei Dati Personali

Prescrizioni relative al trattamento di categorie particolari di dati da parte degli organismi di tipo associativo, delle fondazioni, delle chiese e associazioni o comunità religiose.

Ritenuta compatibile con il GDPR e con il D. Lgs. 101/2018

(norme di adeguamento del Codice della Privacy)

con Provvedimento del Garante del 13.12.2018

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9068972#2

IL PRINCIPIO DI ACCOUNTABILITY

Responsabilizzazione del Titolare
e dei Responsabili del trattamento

Visione «*user-centric*» =
centralità dell'interessato

«*Risk based approach*»

I soggetti

Il titolare del trattamento (art. 4)

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.

Quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

I soggetti

Il responsabile del trattamento

(art. 4)

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

I soggetti

L’incaricato del trattamento

La persona fisica autorizzata a compiere operazioni di trattamento sulla base delle istruzioni ricevute dal Titolare e/o dal Responsabile

I soggetti

Il Data Protection Officer (Responsabile Protezione Dati) Art. 37

La persona designata in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e della prassi in materia di protezione dei dati e della capacità di assolvere i compiti di cui all'art. 39

Il DPO può essere un dipendente del titolare o del responsabile oppure assolvere i suoi compiti in base a un contratto di servizi

IL PRINCIPIO DI ACCOUNTABILITY

Art. 24

1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, **il titolare del trattamento mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento**.

Dette misure sono riesaminate e aggiornate se necessario.

IL PRINCIPIO DI ACCOUNTABILITY

Art. 24

2. Se ciò è proporzionato alle attività di trattamento, le misure di cui al paragrafo 1 includono **l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento**.

3. L'adesione ai codici di condotta di cui all'art. 40 o a un meccanismo di certificazione di cui all'art. 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

CONTITOLARI DEL TRATTAMENTO
Art. 26

Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, **essi sono contitolari del trattamento**. Essi determinano in modo trasparente, **mediante un accordo interno**, le **rispettive responsabilità** in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari sono soggetti.

Art. 25

Privacy By Design

Privacy By Default

PRIVACY BY DESIGN

Risk Based Approach

*Tenendo conto dello **stato dell'arte** e dei **costi di attuazione**, nonché della **natura**, dell'**ambito di applicazione**, del **contesto** e delle **finalità** del trattamento, come anche dei **rischi** aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche…..*

*…**Sia al momento di determinare i mezzi** del trattamento **sia all'atto del trattamento stesso**, il titolare mette in atto **misure tecniche e organizzative adeguate**, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.*

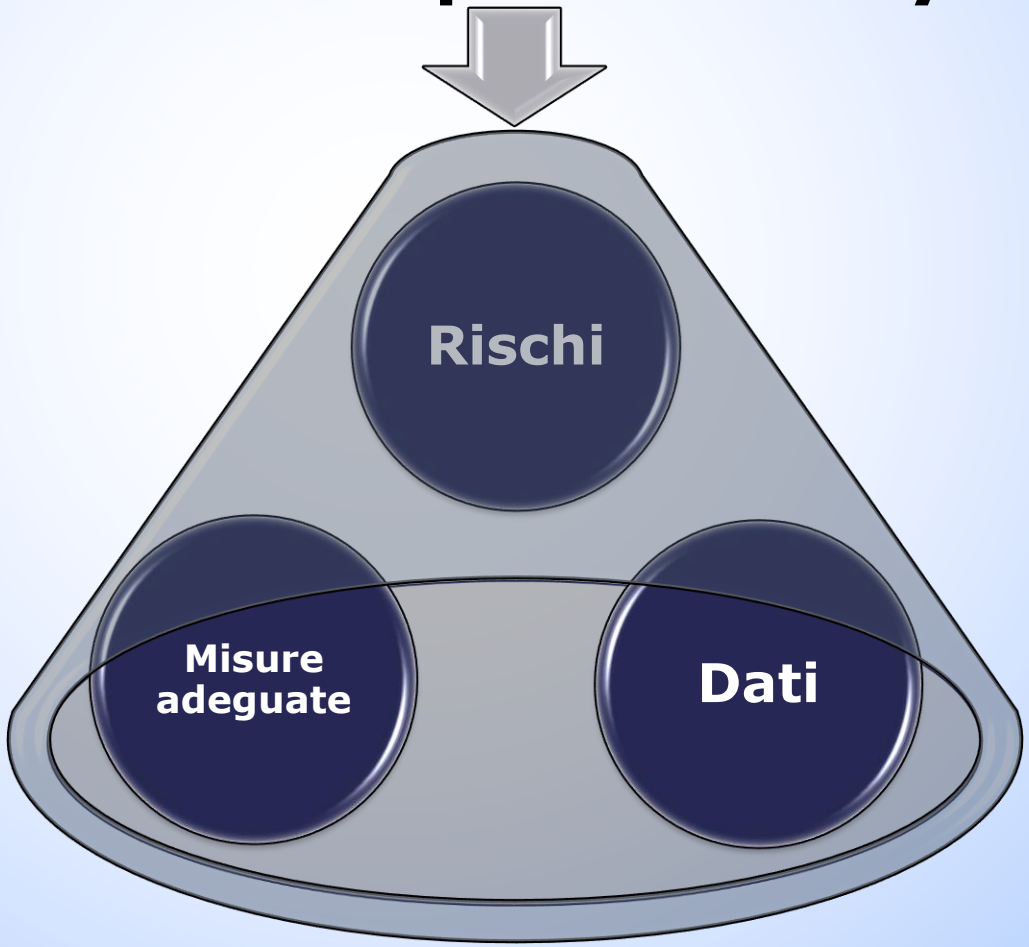
PRIVACY BY DEFAULT

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, **per impostazione predefinita**, solo i dati personali necessari per ogni specifica finalità del trattamento.

Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, **per impostazione predefinita**, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

PRIVACY BY DESIGN: LA DPIA

Data Protection Impact Assessment
(Valutazione Impatto Privacy – VIP)



PRIVACY 4.R

SESSIONE 2

IL GDPR E IL SINDACATO: ADEMPIMENTI, ATTIVITA' E BEST PRACTICE

AVV. ANTONIO LAUDISA
IT MANAGER FRANCESCO ZORZI

STUDIO LEGALE DE VITA

I DATI DEGLI ISCRITTI

I dati identificativi delle persone fisiche che si iscrivono o aderiscono al sindacato rappresentano «dati sensibili»/categorie particolari di dato *ex* art. 9 GDPR.

Nel tempo, il Garante ha a più riprese riconosciuto la particolare tutela del dato, censurando le condotte di diffusione e comunicazione operate molto spesso dai datori di lavoro.

Provv. GPDP 15.11.2018 - Comunicazione dell' iscrizione ad altro sindacato

- Il **datore di lavoro** non può comunicare ad una organizzazione sindacale **la nuova sigla** alla quale ha aderito **un suo ex iscritto**, ma – per adempiere alla procedura di revoca – deve limitarsi a comunicare la non adesione dell'iscritto originario.
- **Il datore può lecitamente trattare questi dati** in base alla legge per adempiere agli obblighi derivanti dal rapporto di lavoro: tra questi rientra il versamento delle quote di iscrizione ad organizzazioni sindacali su delega e per conto del dipendente.
- In questo caso invece ha inviato a tutti i componenti della sigla sindacale una e-mail contenente documenti che riportavano l'iscrizione dei lavoratori ad un altro sindacato.
- **Ciò ha determinato una illecita comunicazione di dati personali sensibili dei reclamanti**.

Data Inventory:
gli altri dati trattati dal sindacato

DATI DEL PERSONALE DIPENDENTE

DATI DI CONSULENTI, COLLABORATORI ESTERNI, FORNITORI

DATI DI SOGGETTI (RAPPRESENTANTI, DIRIGENTI, DELEGATI) DI ALTRE ORGANIZZAZIONI SINDACALI

DATI GIUDIZIARI DI SOGGETTI TERZI (CONTENZIOSO GIUSLAVORISTICO, VERTENZE, ECC.)

Autorizzazione Generale n. 3 del 2016

Si applica ad ass. e org. sindacali, patronati ed a federazioni e confederazioni nelle quali tali soggetti sono riuniti, nel rispetto dello statuto

Sono interessati soci, associati, lavoratori dipendenti di associati e soci rispetto ai dati idonei a rivelare la partecipazione sindacale

Trattamento dei dati particolari per perseguire scopi determinati e legittimi, previsti dalla legge, dallo statuto o dall'atto costitutivo → finalità sindacali

Trattamento per far valere un diritto in sede giudiziaria, amministrativa o di arbitrato, conciliazione quando previsto dalla legge e dai contratti collettivi

Trattamento anche per la tenuta delle scritture contabili, di indirizzari, elenchi e documenti necessari alla gestione amministrativa degli enti

Autorizzazione Generale n. 3 del 2016

Le persone giuridiche, gli enti con scopo di lucro o i liberi professionisti di cui si avvalgono le associazioni per i propri fini, possono trattare i dati degli associati

Questi soggetti terzi (se titolari di autonomo trattamento) ricevono solo i dati particolari indispensabili alle attività di ausilio o gli scopi amministrativi e contabili:

necessario un accordo scritto tra le parti ed un informativa all'interessato

Si possono comunicare i dati personali degli associati, senza consenso dell'interessato, agli altri associati, sempre che ciò sia previsto da statuto/atto costitutivo per il perseguimento di scopi determinati o legittimi e che sia data informativa agli interessati

Nel rispetto dei principi di necessità, finalità e minimizzazione e del regolamento dell'associazione, si deve favorire la consultazione individualizzata, laddove i dati riguardino profili esclusivamente personali dell'associato

Comunicazione esterna all'associazione e diffusione dei dati degli associati/aderenti possono avvenire solo con il consenso dell'interessato, previa informativa su destinatari e finalità, comunque aderenti agli scopi associativi

UNIONI NAZIONALI DI CATEGORIA E UIL CONF.

Confederazione e UNC: soggetti distinti che **condividono finalità** e, talvolta a livello territoriale, mezzi nel trattamento dei **dati degli iscritti**

La contitolarità è garanzia di autonomia dei trattamenti nella condivisione di finalità

(Art. 2 e 3 Statuto Conf.)

L'iscrizione alla UIL avviene tramite la Tessera Confederale, rilasciata dall'UNC a cui ogni soggetto si iscrive (Art. 5,6,7 Statuto Conf.)

UIL e UNC si accordano (ex art. 26) sui rispettivi ruoli e responsabilità: così ogni iscritto, reso edotto dell'accordo, saprà a chi rivolgersi per esercitare i propri diritti

CONTITOLARITA' E ACCORDO INTERNO

- L'**accordo interno** tra contitolari *ex* art. 26 delimita i rispettivi ruoli, rapporti e responsabilità.
- L'accordo dovrà essere reso disponibile agli **interessati**, che in ogni caso potranno **esercitare i propri diritti nei confronti di entrambi i contitolari**.
- La sua **mancata adozione** comporta l'applicazione di una sanzione amministrativa pecuniaria.
- Titolari e Contitolari **rispondono in solido per l'intero ammontare del danno**, al fine di garantire il risarcimento effettivo dell'interessato (salvo il diritto di regresso interno).

Titolare e responsabile del trattamento

- Il titolare individua un responsabile che, per eseguire un **trattamento per conto del "data controller"**, garantisca misure tecniche e organizzative adeguate nel rispetto del Reg. UE (**responsabilità *in eligendo* e *in vigilando*** → **potere di audit**).
- Il responsabile viene individuato in base ad un **atto di designazione scritta** (contratto o altro atto che rispetti i requisiti di cui all'art. 28, comma 3).
- **Il responsabile ha obblighi specifici** derivanti dal Regolamento stesso e che prescindono dalla delega del titolare: **adozione misure ex art. 32, tenuta registro ex art. 30, nomina DPO, ecc**.
- Sulla base dell'art. 28, si dovrebbe ritenere che la figura del **responsabile** sia riferita ad un **soggetto esterno**, diverso invece dal responsabile interno, in precedenza nominato con riferimento alla Legge 196/2003.

I DIRITTI DELL'INTERESSATO

Diritto ad essere correttamente informato (artt. 13-14)

Diritto di accesso (art. 15)

Diritto di rettifica (art. 16)

Diritto all'oblio (art. 17)

Diritto di limitazione del trattamento (art. 18)

Diritto alla portabilità dei dati (art. 20)

Diritto di opposizione (art. 21)

Diritto di non essere sottoposto a trattamento automatizzato (art. 22)

IL DIRITTO ALL'OBLIO E LA TRACCIABILITÀ DEL DATO

La corretta gestione del dato garantisce la sua cancellazione: **il rispetto del diritto all'oblio dipende dall'affidabilità dei sistemi di tracciabilità**

La tracciabilità storica del dato può presentare dei cd. «gap» → responsabilità del titolare

Per garantire la tracciabilità del dato il titolare (o il responsabile) non dovrà solo assicurare la validità dell'infrastruttura ma dovrà **assicurare la corretta gestione del flusso del dato**

Molto spesso le cattive abitudini di chi gestisce materialmente la raccolta e la conservazione dei dati (salvataggio su drive esterni, ecc.) causano l'interruzione della tracciabilità

ADEMPIMENTI: INFORMATIVA

Concisa, trasparente, intellegibile per l'interessato e facilmente accessibile

Scritta con linguaggio semplice e chiaro, resa per iscritto e preferibilmente tramite mezzi elettronici

Il titolare del trattamento agevola l'esercizio dei diritti dell'interessato

INFORMATIVA - CONTENUTO

(Art. 13 – 14 GDPR)

Identità e dati di contatto del titolare e di eventuali contitolari e responsabili

Finalità e base giuridica del trattamento

Destinatari e categorie di destinatari dei dati raccolti

Nei casi *ex* art. 6, par. 1 lett. f), i legittimi interessi del titolare o del terzo su cui si fonda il trattamento

L'intenzione di trasferire i dati raccolti all'estero

Indicazione della nomina di un DPO e dati di contatto

INFORMATIVA - CONTENUTO

(Art. 13 – 14 GDPR)

Periodo di conservazione dei dati o criteri per determinarlo

Diritto di accesso, rettifica e cancellazione dei dati personali

Diritto di limitazione e di opposizione al trattamento, diritto alla portabilità dei dati

Diritto alla revoca del consenso, quando il trattamento sia basato su di esso

Diritto a proporre reclamo all'Autorità Garante

L'obbligo di fornire i dati richiesti e le eventuali conseguenze del diniego

QUANDO FORNIRE L'INFORMATIVA?

Al momento della raccolta, se i dati sono raccolti presso l'interessato o alla prima occasione utile, se i dati pervengono da altra fonte

Se il titolare decide di realizzare un trattamento legittimo, ma estraneo alle finalità descritte nell'informativa, dovrà comunque notiziare l'interessato (c.d. informativa «ulteriore»)

Non c'è obbligo se l'interessato dispone già dell'informazione, se trattamento o comunicazione sono previsti *ex lege,* se si rivela impossibile o richiede uno sforzo sproporzionato

La tutela dell'interessato si realizza con la piena consapevolezza dell'informativa da parte di tutti i soggetti coinvolti nel trattamento (es. incaricato, ecc.)

DIFFERENZA TRA CONSENSO ED INFORMATIVA

L’organizzazione sindacale, sia che raccolga i dati presso l’interessato sia che gli riceva tramite il datore di lavoro, **è tenuta ad informare il proprio iscritto dei trattamenti che effettuerà e dei suoi diritti conseguenti**.

Tuttavia, l’organizzazione sindacale **non ha bisogno del consenso dell’iscritto per tutti quei trattamenti necessari a perseguire le proprie finalità statutarie** e che rientrino nelle ipotesi previste dall’art. 9, comma 2 lett. b) ed d).

SICUREZZA DEL TRATTAMENTO (Art. 32)

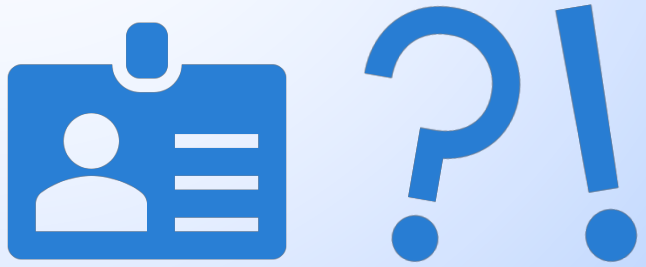
Titolare e responsabile devono mettere in atto misure tecniche e organizzative che garantiscano un livello di sicurezza adeguato al rischio, che ricomprendano:

- ***Pseudonimizzazione e cifratura dei dati***
- ***Riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi di trattamento***
- ***Ripristino tempestivo della disponibilità e dell'accesso dei dati personali in caso di incidente fisico o tecnico***
- ***Procedure per testare, verificare e valutare regolarmente le misure adottate***

SICUREZZA DEL TRATTAMENTO

- Il GDPR non prevede delle misure minime di sicurezza obbligatorie, ma rimette a titolare e responsabile la valutazione sull'idoneità delle misure adottate o da adottare, in base all'analisi del rischio.

- **<u>Come proteggo i dati dei miei iscritti</u>?**



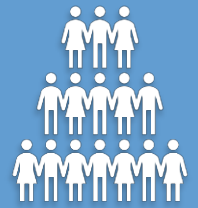
STRUMENTI

Analisi del rischio privacy

Adozione di meccanismi di certificazione

Adesione a codici di condotta

ANALISI DEL RISCHIO



Tipi di dati trattati e di interessati coinvolti, natura dei trattamenti effettuati

Soggetti coinvolti e modalità di raccolta, gestione, conservazione del dato → un corretto audit di tutti gli incaricati consente di stabilire l'effettivo flusso dei dati

Natura, contesto, ambito e finalità del trattamento:

rischio o un «rischio elevato»

Furto o usurpazione di identità

Trattamento di dati ex art. 9 GDPR

Pregiudizio alla reputazione

Trattamento di dati giudiziari ex art. 10 GDPR

Perdita di riservatezza dei dati coperti da segreto professionale

Rischio connesso ad interessati vulnerabili (i minori)

*Cfr. GDPR Cons. 75

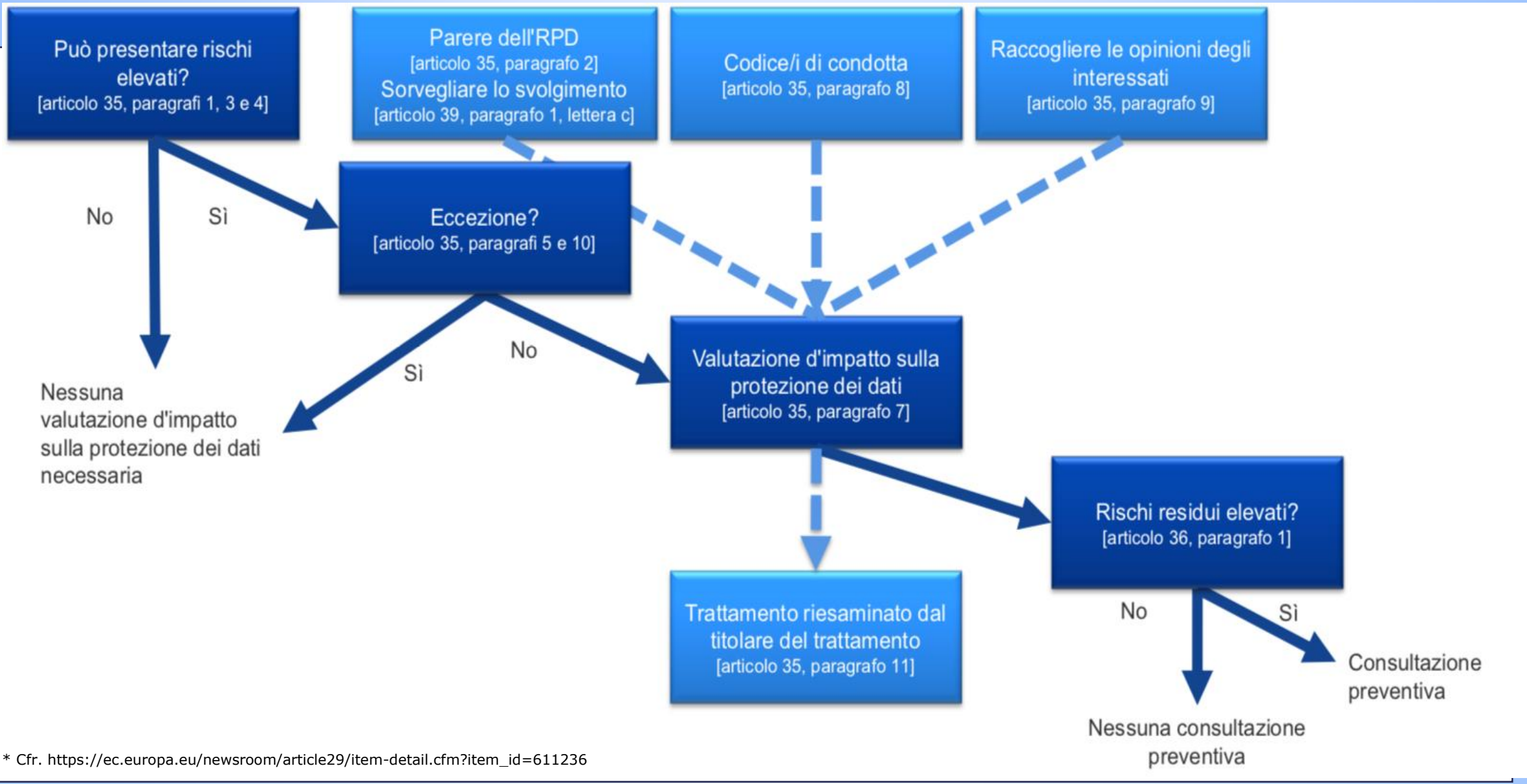
PRINCIPALI TIPOLOGIE DI RISCHIO

DPIA: OBBLIGO O FACOLTÀ?

È necessario eseguire una DPIA solo se il trattamento può presentare un **rischio elevato** per diritti e libertà delle persone fisiche

Per misurare il «rischio elevato» il WP29 ha previsto nove diversi criteri: in costanza di due o più di essi, il titolare deve concretamente valutare di ricorrere alla DPIA

A prescindere dalla DPIA, rimane l'obbligo del titolare di adottare le misure necessarie a gestire i rischi per diritti e libertà: in caso di dubbio, il WP29 raccomanda di eseguire comunque la DPIA



* Cfr. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

DPIA: QUANDO È NECESSARIO EFFETTUARLA?

«DATA BREACH» E NOTIFICA DELLA VIOLAZIONE ALL'ANC

Descrivere la natura della violazione dei dati, delle categorie e del numero approssimativo di interessati in questione nonché delle categorie e del numero di registrazioni di dati coinvolte

Comunicare nome e dati di contatto del DPO o di altro punto di contatto presso cui ottenere informazioni

Descrivere le probabili conseguenze della violazione

Descrivere le misure adottate o proporre quelle da adottare per porre rimedio alla violazione dei dati o almeno per limitarne gli effetti

La segnalazione all'Autorità Garante dovrà essere effettuata entro 72 ore o, laddove non sia possibile, comunque senza ingiustificato ritardo

NOTIFICAZIONE DI «DATA BREACH» ALL'INTERESSATO

Se c'è un rischio elevato per i diritti e le libertà dell'interessato, il titolare del trattamento notifica senza ritardo la violazione allo stesso

Il titolare indica i dati di contatto del DPO, descrive le probabili conseguenze della violazione e indica le misure adottate o da adottare per rimediare alla violazione o limitarne gli effetti

Il titolare può omettere la notificazione, quando abbia adottato misure tecniche adeguate, quali la cifratura dei dati violati; quando abbia adottato misure idonee a scongiurare il «rischio elevato»; quando la comunicazione richiederebbe sforzi sproporzionati.

«DATA BREACH» E MECCANISMO DI SEGNALAZIONE

REGISTRO EX ART. 30 - CONTENUTO

Nome e dati di contatto del titolare, dei contitolari, di responsabili e sub-responsabili e del DPO

Finalità e base giuridica del trattamento

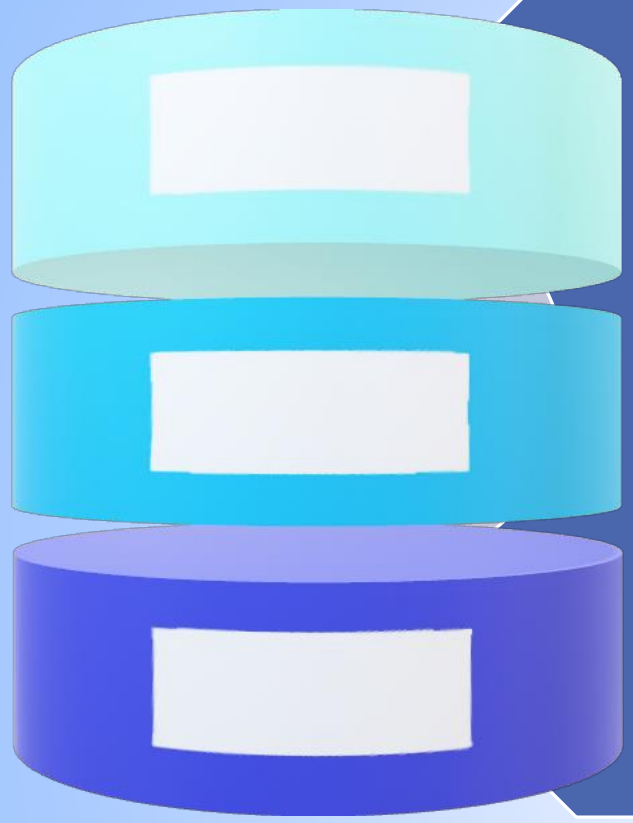
Descrizione di categorie di interessati e dei dati personali trattati

Descrizione dei destinatari (anche di Paese Terzo se previsti) cui i dati verranno comunicati

Termine per cancellazione dei dati (dove prevedibile)

Descrizione delle misure di sicurezza ex art. 32 adottate

Anche il responsabile del trattamento redige un registro, in cui sono riportate, tra gli altri, le categorie di trattamenti effettuati per conto di singolo titolare e le misure di sicurezza adottate ex art. 32 (cfr. Art. 30, par. 2)



Imprese ed organizzazioni con meno di 250 dipendenti non sono obbligate a tenere il registro, a meno che il trattamento:

- presenti un rischio per diritti e libertà dell'interessato;

- non sia occasionale;

- **includa il trattamento di categorie particolari di dati ex art. 9** o di dati relativi a condanne penali ex art. 10 GDPR.

Le organizzazioni sindacali, dunque, sono tenute a redigere il registro ex art. 30 GDPR*.

IL REGISTRO DEI TRATTAMENTI (ART.30): OBBLIGO O FACOLTÀ?

https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento

IL REGISTRO DEI TRATTAMENTI: FINALITÀ

Il registro del trattamento è uno dei principali elementi di «accountability» del titolare: non è un semplice adempimento formale ma costituisce **parte integrante di un sistema di corretta gestione dei dati personali.** Esso deve avere forma scritta e deve essere esibito su richiesta del Garante: così favorisce la verifica sulla rigorosa adozione delle misure e permette un'analisi tempestiva dei rischi.

REGISTRO DEI TRATTAMENTI:

BEST PRACTICE

Il registro deve avere un aggiornamento costante, poiché il suo contenuto deve corrispondere all'effettività dei trattamenti

Deve riportare la data di creazione in maniera verificabile o la data di inserimento di nuove schede di trattamento, assieme alla data di ultimo aggiornamento

Molto spesso, nella prassi, è il DPO a tenere il registro del trattamento: questa abitudine è riconosciuta ed ammessa dal Garante e dall'EDPB, purché sia chiaro che la **responsabilità rimane del titolare/responsabile**

L’incaricato è il primo soggetto che garantisce la corretta acquisizione dei dati

È il punto di partenza (e di vulnerabilità) nella tracciabilità dei dati

Può assicurare una tempestiva segnalazione dell’anomalia

(pre-data breach)

L’INCARICATO:

RUOLO E RISCHI

IL DATA PROTECTION OFFICER

Tutte le organizzazioni sindacali sono tenute a nominare un DPO, come segnalato dal GPDP, poiché la loro attività principale consiste nel trattamento su larga scala di dati *ex* art. 9 GDPR

Il DPO può essere un interno (individuato con nomina formale) oppure un esterno che operi in base ad un contratto di servizi

Il DPO deve avere la disponibilità di tutte le risorse umane e finanziarie per svolgere i propri compiti e non deve ricevere istruzioni, né penalizzazioni per la sua attività. Non deve essere essere in conflitto di interessi → **AUTONOMIA ED INDIPENDENZA**

Il titolare o il responsabile del trattamento deve pubblicare i dati di contatto del DPO e, soprattutto, deve comunicare formalmente la sua nomina all'autortià di controllo

I COMPITI DEL DPO

Informa e fornisce consulenza a tutti i soggetti coinvolti nel trattamento sulle prescrizioni del GDPR e della normativa UE e nazionale in materia

Sorveglia l'applicazione del GDPR e delle normative UE e nazionali in materia, curandosi che titolare/responsabile si dedichino alla formazione del personale

Può fornire un parere in merito alla DPIA, se richiesto

Coopera con l'autorità Garante e funge da punto di contatto con la stessa

N.B.: l'elenco riportato dal GDPR non è tassativo!

DATA PROTECTION OFFICER : BEST PRACTICE

Ogni UNC dovrebbe nominare il proprio DPO: la logica del «gruppo di imprese» (nomina di un unico DPO della controllante per tutte le controllate) non è applicabile ai rapporti tra Confederazioni e UNC

In ogni caso si raccomanda che **il punto di contatto** con interessati e Garante sia comunque **una persona fisica**

Il DPO nominato **non deve avere incarichi di alta direzione** (il segr. Gen., il segr. Org., ecc.) **oppure una posizione tale da poter determinare mezzi e finalità del trattamento** (il tesoriere, il responsabile IT, ecc.)

Quando si tratti di **dipendente**, il DPO dovrà essere una **persona fisica**; nel caso di soggetto **esterno**, potrà essere una **persona giuridica**

DATA PROTECTION OFFICER: BEST PRACTICE

Il DPO è un controllore e revisore indipendente

Svolge un incarico dinamico, in cui deve essere coadiuvato dai soggetti che si occupano del trattamento (soprattutto dagli incaricati)

La sinergia tra DPO e autori del trattamento consente la verifica del corretto funzionamento delle procedure

In caso contrario, il DPO segnalerà al titolare o al dipartimento di *compliance* preposto le criticità riscontrate

PRIVACY 4.R

SESSIONE 3

TUTELA DELL'INTERESSATO, RESPONSABILITÀ E SANZIONI

AVV. VALENTINA GUERRISI

STUDIO LEGALE DE VITA

I DIRITTI DELL'INTERESSATO

Diritto ad essere correttamente informato (artt. 13-14)

Diritto di accesso (art. 15)

Diritto di rettifica (art. 16)

Diritto all'oblio (art. 17)

Diritto di limitazione del trattamento (art. 18)

Diritto alla portabilità dei dati (art. 20)

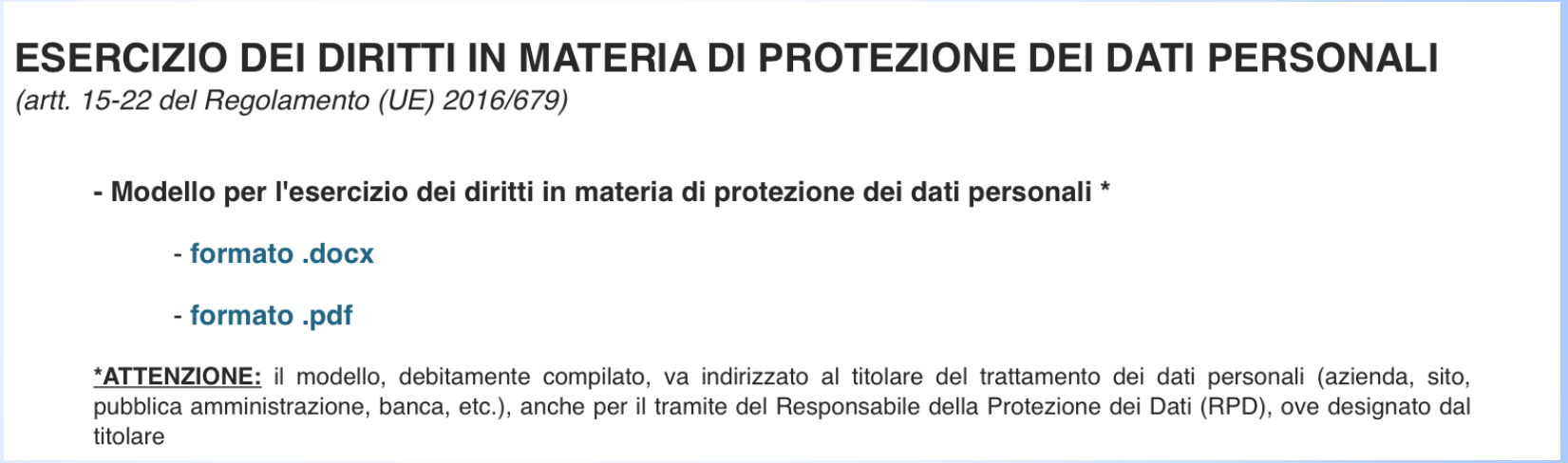
Diritto di opposizione (art. 21)

Diritto di non essere sottoposto a trattamento automatizzato (art. 22)

COME SI ESERCITANO I DIRITTI?

- L'interessato può presentare al titolare un'**istanza**, senza particolari formalità per effettuare la sua richiesta (accesso, rettifica, cancellazione etc.).

  Es. Modulo predisposto dal Garante*:



ESERCIZIO DEI DIRITTI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

(artt. 15-22 del Regolamento (UE) 2016/679)

- Modello per l'esercizio dei diritti in materia di protezione dei dati personali *

- formato .docx

- formato .pdf

***ATTENZIONE:** il modello, debitamente compilato, va indirizzato al titolare del trattamento dei dati personali (azienda, sito, pubblica amministrazione, banca, etc.), anche per il tramite del Responsabile della Protezione dei Dati (RPD), ove designato dal titolare

- Il titolare deve fornire risposta **entro 1 mese** dal suo ricevimento.
- Il termine prorogabile di 2 mesi qualora necessario per la complessità e il numero delle richieste, ma l'interessato deve essere informato di tale proroga entro il primo mese.

*https://www.garanteprivacy.it/home/modulistica-e-servizi-online

I RIMEDI PER L'INTERESSATO

Diritto di denunciare all'Autorità Nazionale di Controllo (ANC – art. 77)

Diritto di presentare ricorso giurisdizionale (artt. 78 - 79)

Diritto al risarcimento del danno (art. 82)

IL RECLAMO ALL'ANC
Art. 77 GDPR
(Art. 142 Codice Privacy)

- Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento che lo riguarda violi il presente regolamento, ha il **diritto di proporre reclamo a un'autorità di controllo**, segnatamente nello Stato membro in cui risiede abitualmente, lavora oppure del luogo in cui si è verificata la presunta violazione.
- **L'autorità di controllo a cui è stato proposto il reclamo informa il reclamante dello stato o dell'esito del reclamo**, compresa la possibilità di un ricorso giurisdizionale ai sensi dell'articolo 78.

IL RICORSO GIURISDIZIONALE

Art. 78

L'interessato può proporre **ricorso giurisdizionale contro l'ANC** se:

- non è soddisfatto della sua decisione (che è giuridicamente vincolante)
- l'ANC non ha trattato il reclamo o non ha informato l'interessato dello stato dell'istruttoria o del suo esito.

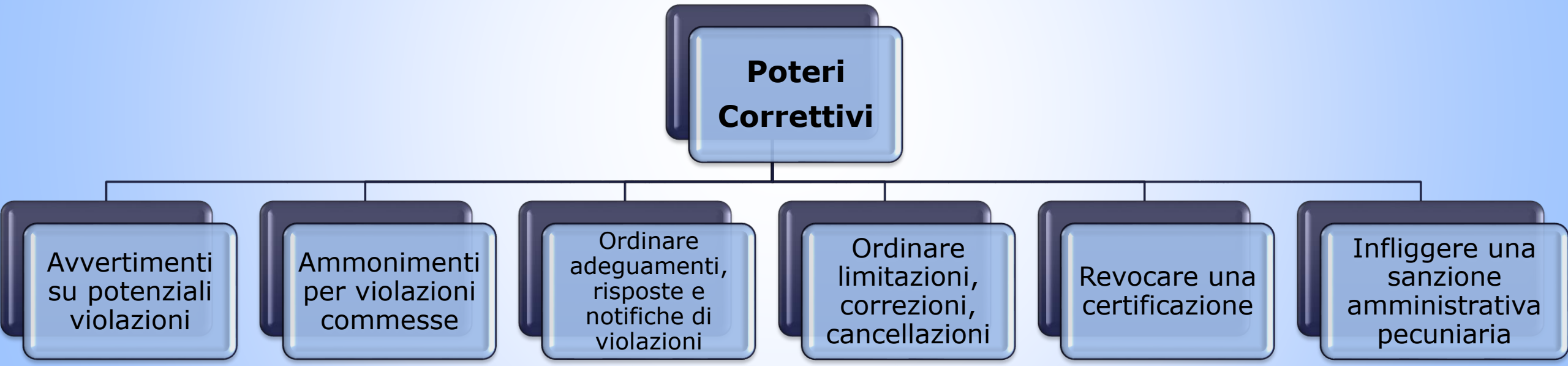
Art. 79

L'interessato può proporre ricorso giurisdizionale **contro il titolare/responsabile** se ritiene che i suoi diritti siano stati violati a seguito di trattamento.

I POTERI DELL'ANC
Art. 58 GDPR

*** Cfr. Artt. 157 e ss. Codice Privacy**

I POTERI DELL'ANC
Art. 58



I POTERI DELL'ANC
Art. 58 GDPR

DIRITTO AL RISARCIMENTO E RESPONSABILITÀ Art. 82

- Chiunque subisca **un danno materiale o immateriale** causato da una violazione del presente regolamento ha il diritto di ottenere il **risarcimento** del danno **dal titolare del trattamento o dal responsabile del trattamento**.

DIRITTO AL RISARCIMENTO E RESPONSABILITÀ
Art. 82

Il **titolare** risponde per il danno cagionato dal suo **trattamento che violi il GDPR**

Il **responsabile risponde** per il danno causato dal trattamento **solo se**:

- non ha adempiuto agli obblighi del GDPR specificamente diretti ai responsabili
- ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare

Il titolare e il responsabile sono esonerati dalla responsabilità se dimostrano che l'evento dannoso non gli è in alcun modo imputabile

DIRITTO AL RISARCIMENTO E RESPONSABILITÀ Art. 82

- Titolari/Contitolari e Responsabili **rispondono in solido per l'intero ammontare del danno**, al fine di garantire il risarcimento effettivo dell'interessato (salvo il diritto di regresso interno).
- L'**accordo interno** tra Contitolari ex art. 26 GDPR delimita i rispettivi ruoli, rapporti e responsabilità.
- La sua **mancata adozione** comporta l'applicazione di una sanzione amministrativa pecuniaria.

LE SANZIONI AMMINISTRATIVE PECUNIARIE
Art. 83 GDPR

LE SANZIONI AMMINISTRATIVE PECUNIARIE
Art. 83 GDPR

Fino a **10 milioni di Euro** oppure, per le imprese, fino al **2% del fatturato mondiale totale annuo** se la violazione riguarda:

- Gli obblighi previsti per il titolare e il responsabile del trattamento *ex* artt. 8, 11, da 25 a 39, 42 e 43
- Gli obblighi dell'organismo di certificazione
- Gli obblighi dell'organismo di controllo

LE SANZIONI AMMINISTRATIVE PECUNIARIE
Art. 83 GDPR

Fino a **20 milioni di Euro** oppure, per le imprese, fino al **4% del fatturato mondiale totale annuo** se la violazione riguarda:

- I princìpi di base del trattamento, comprese le condizioni relative al consenso
- I diritti degli interessati
- I trasferimenti di dati a un destinatario in un paese terzo o organizzazione internazionale
- Qualsiasi obbligo di legge degli Stati membri o l'inosservanza di un ordine dell'ANC o il negato accesso

CONDIZIONI DI APPLICAZIONE
Art. 83 GDPR

- **Natura, gravità e durata della violazione**
- **Dolo o colpa della violazione**
- **Misure adottate per attenuare il danno**
- **Grado di responsabilità di titolare e responsabile**
- **Eventuali precedenti violazioni**
- **Cooperazione con l'ANC per rimediare e attenuare effetti negativi**
- **Categoria di dati oggetto di violazione**
- **Modalità con le quali l'ANC è venuta a conoscenza della violazione**
- **Adesione a codici di condotta o certificazioni**
- **Rispetto di precedenti provvedimenti dell'ANC**
- **Altri fattori attenuanti o aggravanti**

PROCEDIMENTO SANZIONATORIO
(Art. 166 Codice Privacy)

In caso di violazione viene avviato il procedimento

Può essere avviato sia nei confronti di privati che di autorità ed organismi pubblici

L'avvio del procedimento viene notificato al titolare e/o al responsabile

Entro 30 gg il titolare può inviare scritti difensivi, documenti e chiedere di essere sentito

L'ANC emette il provvedimento sanzionatorio

Entro 30 gg il titolare può adeguarsi alle direttive e definire con il pagamento di metà della sanzione

Oppure entro 30 gg può presentare ricorso all'AG

ILLECITI PENALI
Art. 167 Codice Privacy
Trattamento illecito di dati

1. **Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione degli articoli 123 (dati relativi al traffico delle comunicazioni), 126 (dati relativi all'ubicazione), 130 (comunicazioni indesiderate) o del provvedimento di cui all'art. 129 (elenchi dei contraenti) arreca nocumento all'interessato, è punito con la reclusione da 6 mesi a un anno e 6 mesi.**

ILLECITI PENALI
Art. 167 Codice Privacy
Trattamento illecito di dati

2. **Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del GDPR in violazione delle disposizioni di cui agli artt. 2-*sexies* (trattamento per motivi di interesse pubblico) e 2-*octies* (dati su condanne penali e reati), o delle misure di garanzia di cui all'art. 2-*septies* (dati genetici, biometrici e di salute) ovvero operando in violazione delle misure adottate ai sensi dell'articolo 2-*quinquiesdecies* (trattamento con rischi elevati per motivo di interesse pubblico), arreca nocumento all'interessato, è punito con la reclusione da 1 a 3 anni.**

ILLECITI PENALI
Art. 167 Codice Privacy
Trattamento illecito di dati

3. **Salvo che il fatto costituisca più grave reato, la pena di cui al comma 2 si applica anche a chi, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti, arreca nocumento all'interessato.**

ILLECITI PENALI

Art. 167 *bis* Codice Privacy

COMUNICAZIONE E DIFFUSIONE ILLECITA DI DATI PERSONALI OGGETTO DI TRATTAMENTO SU LARGA SCALA

È punito con la reclusione **da 1 a 6 anni** chi, al fine di trarre profitto o arrecare danno:

1. **Comunica o diffonde un archivio automatizzato** o una parte sostanziale di esso **contenente dati personali oggetto di trattamento su larga scala**, in violazione degli articoli 2-*ter*, 2-*sexies* e 2-*octies*
2. Comunica o diffonde, senza consenso, un archivio automatizzato o parte sostanziale di esso contenete dati personali oggetto di trattamento su larga scala, quando il consenso dell'interessato è richiesto per la comunicazione e diffusione.

ILLECITI PENALI
Art. 167-*ter*

ACQUISIZIONE FRAUDOLENTA DI DATO PERSONALI OGGETTO DI TRATTAMENTO SU LARGA SCALA

Salvo che il fatto costituisca più grave reato, chiunque al fine di trarne profitto per sé o per altri, ovvero di arrecare danno, **acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso** contenente dati personali oggetto di trattamento su larga scala è punito con la reclusione **da 1 a 4 anni**.

ILLECITI PENALI

Art. 168

FALSITÀ NELLE DICHIARAZIONI AL GARANTE E INTERRUZIONE DELL'ESECUZIONE DEI COMPITI O DELL'ESERCIZIO DEI POTERI DEL GARANTE

1. Salvo che il fatto costituisca più grave reato, chiunque, in un procedimento o nel corso di accertamenti dinanzi al Garante, **dichiara o attesta falsamente notizie o circostanze o produce atti e documenti falsi**, è punito con la reclusione **da 6 mesi a 3 anni**.
2. Fuori dei casi di cui al comma 1, è punito con la reclusione **sino ad 1 anno** chiunque intenzionalmente cagiona un'interruzione o turba la regolarità di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti.

ILLECITI PENALI
Art. 170

INOSSERVANZA DEI PROVVEDIMENTI DEL GARANTE

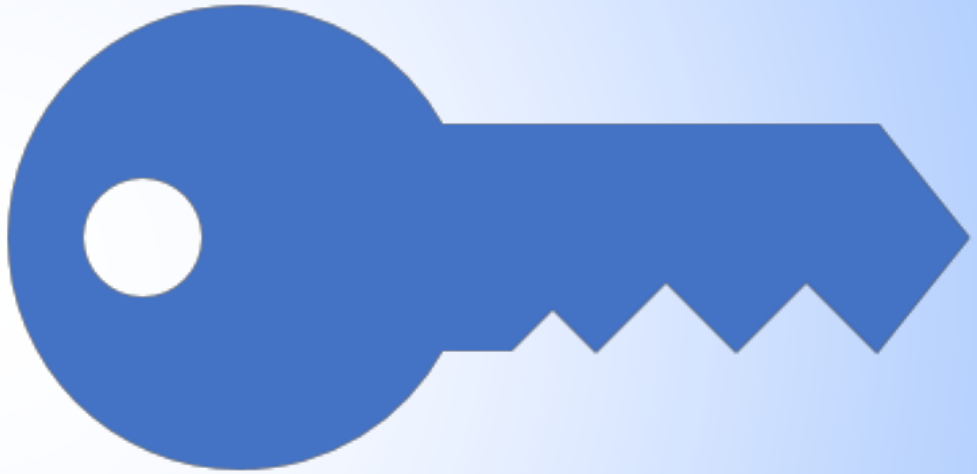
Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi:

- dell'articolo 58, par. 2, lett. f) del GDPR (limitazioni o divieti di trattamento);
- dell'art. 2-*septies*, comma 1, Codice Privacy (dati genetici, biometrici e di salute);
- nonché i provvedimenti generali

è punito con la **reclusione da 3 mesi a 2 anni**.

PRIVACY 4.R:

Regolamento
Ruoli
Rischi
Responsabilità



Roma, 18 Aprile 2019

Studio Legale De Vita