Percorso integrato

Regolamento europeo per la protezione dei dati (GDPR)

Regolamento Europeo sulla Protezione dei Dati: la nuova normativa in materia di protezione dei dati e gli impatti sulle procedure e sull'organizzazione

Cagliari - 4 aprile 2018
ore 9.30 - 13.30

Avv. Giovanni Battista Gallus - Avv. Francesco Paolo Micozzi

MENU

- I principi introdotti dal Nuovo Regolamento Europeo sulla Protezione dei Dati;
- I soggetti;
- Il dato personale e il suo trattamento;
- L'informativa;
- Accountability;
- Il Responsabile della Protezione dei Dati – (RPD o DPO, Data Protection Officer);
- Registri delle attività di trattamento;
- Data protection "by design" e "by default";
- La Valutazione d'impatto sulla protezione dei dati (DPIA);
- Sicurezza dei dati personali;
- Notifica in caso di violazione dei dati personali (data breach);
- Protezione dei dati personali e trasparenza PA;
- Mezzi di ricorso, responsabilità e sanzioni;

Disclaimer

A tutt'oggi non è stato ancora reso disponibile il testo (se non in bozza e versione non ufficiale) del decreto legislativo che il Governo dovrà emanare entro il prossimo 21 maggio nel rispetto della delega che il Parlamento ha concesso con l'art. 13 della L. 163/2017 per adeguare il vigente codice della privacy al GDPR.

Introduzione

Perché il GDPR?

Considerando 6 - La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività

Considerando 13 - Per assicurare un livello coerente di protezione delle persone fisiche in tutta l'Unione e prevenire disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno, **è necessario un regolamento che garantisca certezza del diritto e trasparenza** ...

Trattamenti esclusi (art. 2 GDPR)

- **di dati “non personali”**
- **effettuati per attività che non rientrano nell’ambito di applicazione del diritto dell’Unione** (art. 5, co. 2 Trattato sull’Unione Europea)
- **effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE;**
- **effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;**
- **effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.**

Ambito territoriale di applicazione (art. 3 GDPR)

1) Titolare o responsabile stabilito in UE a prescindere dal luogo in cui è effettuato il trattamento

2) Interessati si trovano in UE ma titolare o responsabile non stabilito in UE se i trattamenti riguardano:

a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione; oppure
b) il monitoraggio del comportamento degli interessati che abbia luogo nell'UE

3) Titolare non stabilito in UE, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico.

“Stabilimento principale”

per quanto riguarda un **titolare del trattamento** con stabilimenti in più di uno Stato membro, il **luogo della sua amministrazione centrale nell'Unione**, **salvo che** le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;

con riferimento a un **responsabile del trattamento** con stabilimenti in più di uno Stato membro, il **luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento** nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

Il dato personale e il suo trattamento

ARRAY

Avv. Giovanni Battista Gallus - Avv. Francesco Paolo Micozzi

Il dato personale, perno del GDPR

«**dato personale**»: qualsiasi informazione riguardante una **persona fisica identificata o identificabile** («interessato»); 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;

I principi generali - l'art. 5

1. I dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (**«liceità, correttezza e trasparenza**»);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; [...] (**«limitazione della finalità»**);

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (**«minimizzazione dei dati»**);

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (**«esattezza»**);

I principi generali - l'art. 5

e) 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; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato (**«limitazione della conservazione»**);

f) 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 (**«integrità e riservatezza**»).

2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo (**«responsabilizzazione»**).

Responsabilizzazione (accountability)

Dicesi accountability…

Protezione dei dati: obbligo e opportunità

"Non mi interessa la disciplina sulla protezione dei dati personali, ditemi soltanto cosa dobbiamo fare, quali adempimenti, quale check-list e quanti soldi dobbiamo impiegare"

non è più una soluzione percorribile: l'accountability lo esclude

In sintesi

Accountability

Misure adeguate e efficaci per garantire i principi e gli obblighi

Adattabilità

Dimostrazione dell'osservanza degli obblighi

One size fits all?

*"**Non esistono alternative valide alle soluzioni "su misura"**. Infatti, le misure specifiche da applicare devono essere determinate in funzione dei fatti e delle circostanze di ciascun caso specifico, con particolare attenzione al rischio inerente al trattamento e al tipo di dati. **Un approccio uguale per tutti** avrebbe il solo effetto di costringere i responsabili del trattamento all'interno di strutture inadatte e **si rivelerebbe** quindi **fallimentare**"*

Art. 29WP, Parere 3/2010 - WP 173

Accountability nel GDPR

Considerando 74

(74) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.

(74) È opportuno stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. In particolare, il titolare del trattamento dovrebbe essere tenuto a **mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento**, compresa l'efficacia delle misure. Tali misure dovrebbero tener conto della **natura**, dell'**ambito di applicazione**, del **contesto** e delle **finalità** del trattamento, nonché del **rischio per i diritti e le libertà** delle persone fisiche.

Un principio “distribuito”

Art. 5 par. 2. - Principles relating to processing of personal data

The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).

2. Il titolare del trattamento **è competente** per il rispetto del paragrafo 1 **e in grado di comprovarlo** («responsabilizzazione»)

Art. 24 par. 1 - Responsibility of the controller

Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

Responsabilità del titolare del trattamento

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 e 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 qualora necessario.

I soggetti e la governance della protezione dei dati personali

ARRAY

Avv. Giovanni Battista Gallus - Avv. Francesco Paolo Micozzi

Come si dice in...

Italiano	Inglese	Francese
Titolare	Controller	Responsable du traitement
Responsabile del trattamento	Processor	Sous-traitant
Responsabile della protezione dei dati	Data Protection Officer	Délégué à la protection des données
Interessato	Data subject	Personne concernée
Autorità di controllo	Supervisory authority	Autorité de contrôle

Le figure soggettive - Titolare e contitolari

Art. 4, n. 7 - **«titolare del trattamento»**: 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;

Art. 26 - **Contitolari**: due o più titolari del trattamento che determinano congiuntamente le finalità e i mezzi del trattamento

Le figure soggettive - Titolare e contitolari

La qualifica di Titolare del trattamento non è prevista per "attribuzione" normativa ma discende da una **situazione di fatto**, dal rapporto tra il soggetto e i dati personali.

Art. 4 n. 8 GDPR - **«responsabile del trattamento»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo **che tratta dati personali** per conto del titolare del trattamento;

Art. 4 comma 1 lett. g D.lgs 196/2003 - "responsabile", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo **preposti dal titolare al trattamento** di dati personali;

Non confondiamo questa figura con il **Responsabile della protezione dei dati** - RPD (o data protection officer - DPO), disciplinato dagli artt. 37–39 del GDPR

Il "nuovo" art. 29 D.lgs 196/2003

1. Il responsabile è designato dal titolare **facoltativamente**.

2. Se designato, il responsabile è **individuato** tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

3. Ove necessario per esigenze organizzative, possono essere designati responsabili **più soggetti**, anche mediante suddivisione di compiti.

4. I **compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare.**

Il “nuovo” art. 29 D.lgs 196/2003

4-bis. Fermo restando quanto previsto ai commi 1, 2, 3 e 4, il titolare può avvalersi, per il trattamento di dati, anche sensibili, di **soggetti pubblici o privati** che, in qualità di responsabili del trattamento, forniscano le garanzie di cui al comma 2. I titolari stipulano con i predetti responsabili atti giuridici in forma scritta, che specificano la **finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le modalità di trattamento**; i predetti atti **sono adottati in conformità a schemi tipo predisposti dal Garante**.

5. Il responsabile effettua il trattamento attenendosi alle condizioni stabilite ai sensi del comma 4-bis e alle istruzioni impartite dal titolare, **il quale, anche tramite verifiche periodiche**, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2, delle proprie istruzioni e di quanto stabilito negli atti di cui al comma 4-bis.

Quale spazio per la nomina del “responsabile interno”?

Gli “incaricati” - art. 29 - Trattamento sotto l’autorità del titolare del trattamento o del responsabile del trattamento

Art. 29. Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell’Unione o degli Stati membri.

Art. 32 n. 4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti 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.

Dovremmo chiamarli “Autorizzati al trattamento”?

La gestione delle figure soggettive

- **Individuare i trattamenti dei quali la RAS sia titolare**
- **Individuare eventuali situazioni di contitolarità e provvedere a regolamentarle**
- **Individuare i responsabili esterni, e provvedere a regolamentare i rapporti ex art. 28 GDPR**
- **Costruire un organigramma privacy coerente, definendo ruoli e responsabilità**
- **Istruire gli "incaricati" del trattamento**
- **Coordinare il quadro soggettivo con la nuova figura del DPO**
- **Documentare l'intero processo**

Informativa

Considerando 61

L'interessato **dovrebbe ricevere le informazioni** relative al trattamento di dati personali che lo riguardano **al momento della raccolta presso l'interessato o**, se i dati sono ottenuti da altra fonte, **entro un termine ragionevole**, in funzione delle circostanze del caso.

In cosa resta uguale ad oggi?

- **Se i dati sono raccolti presso l'interessato l'informativa deve precedere il trattamento**
- **Se i dati non sono raccolti presso l'interessato l'informativa deve indicare le categorie dei dati personali oggetto di trattamento**
- **Il Titolare deve indicare i propri dati e quelli dell'eventuale rappresentante nel territorio italiano**
- **Deve indicare le finalità del trattamento**
- **Deve indicare i diritti dell'interessato**
- **Deve indicare l'eventuale responsabile del trattamento (data processor)**
- **Deve indicare i destinatari dei dati**

Come cambia l'informativa nel GDPR?

Contenuti

- **Dati di contatto del Data Protection Officer**
- **Base giuridica del trattamento**
- **Interesse legittimo al trattamento** (non applicabile alle PA)
- **Indicazione se sia previsto il trasferimento di dati in Paesi terzi**
  - **in caso affermativo: attraverso quali strumenti**
- **Periodo di conservazione dei dati**
  - **Nel caso non possa indicarsi il periodo preciso si dovrà, almeno, indicare i criteri stabiliti per stabilire la durata della conservazione**
- **Il diritto di presentare reclamo all'Autorità di controllo**
- **Si deve specificare se il trattamento comporta processi decisionali automatizzati e, nel caso, la logica dei processi decisionali e le possibili conseguenze per l'interessato**

I Registri delle attività di trattamento

ARRAY

Avv. Giovanni Battista Gallus - Avv. Francesco Paolo Micozzi

Considerando 82

Per **dimostrare che si conforma al presente regolamento**, il titolare del trattamento o il responsabile del trattamento **dovrebbe tenere un registro delle attività di trattamento effettuate sotto la sua responsabilità**. Sarebbe necessario obbligare tutti i titolari del trattamento e i responsabili del trattamento a cooperare con l'autorità di controllo e a mettere, su richiesta, detti registri a sua disposizione affinché possano servire per monitorare detti trattamenti.

In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations

Il registro del Titolare – art. 30.1

1. Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

a) il **nome e i dati di contatto del titolare del trattamento** e, ove applicabile, **del contitolare** del trattamento, **del rappresentante** del titolare del trattamento e **del responsabile della protezione dei dati**;

b) le **finalità** del trattamento;

c) una descrizione delle **categorie di interessati e delle categorie di dati personali**;

d) le **categorie di destinatari** a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

f) ove possibile, i **termini ultimi previsti per la cancellazione** delle diverse categorie di dati;

g) ove possibile, una **descrizione generale delle misure di sicurezza tecniche e organizzative** di cui all'articolo 32, paragrafo 1.

Le formalità e l'aggiornamento

3. I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.

4. **Su richiesta**, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento **mettono il registro a disposizione dell'autorità di controllo**.

I registri vanno aggiornati?

Il Garante e il Registro dei trattamenti

Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico – **indispensabile per ogni valutazione e analisi del rischio**. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

RACCOMANDAZIONI

La tenuta del registro dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema di corretta gestione dei dati personali. Per tale motivo, si invitano tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro e, in ogni caso, a compiere un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche – ove già non condotta. **I contenuti del registro sono fissati, come detto, nell'art. 30; tuttavia, niente vieta a un titolare o responsabile di inserire ulteriori informazioni se lo si riterrà opportuno proprio nell'ottica della complessiva valutazione di impatto** dei trattamenti svolti.

Nello specifico, si richiama l'attenzione sulla sostanziale coincidenza fra i contenuti della notifica dei trattamenti di cui all'art. 38 del Codice e quelli che devono costituire il registro dei trattamenti ex art. 30 regolamento; l'Autorità sta valutando di mettere a disposizione un modello di registro dei trattamenti sul proprio sito, che i singoli titolari potranno integrare nei modi opportuni.

CPVP
Commission de la protection de la vie privée

Plan du site • Lexique • FAQ • Presse • Liens • Contact •

NL • FN • FR

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES ("GDPR") NEW

THÈMES DE VIE PRIVÉE
Nos activités quotidiennes

LÉGISLATION ET NORMES
Textes de référence relatifs à la protection des données

DÉCISIONS
Nos avis, autorisations et recommandations

PUBLICATIONS
Les publications de la Commission vie privée

À PROPOS DE LA CPVP
Pour en savoir plus sur la Commission vie privée

Accueil › Modèle de Registre des activités de traitement

Modèle de Registre des activités de traitement

La Commission vie privée met à disposition un modèle de Registre destiné aux responsables de traitements afin d'aider les entreprises et organismes à établir un Registre des activités de traitement.

Comment compléter le Registre ?

Le modèle de registre que nous proposons contient plus d'informations que ce que le RGPD ne requiert. Ce modèle de Registre doit donc être considéré comme un réel outil car il permet à l'utilisateur de garder une vue d'ensemble sur d'autres informations qui ont également une importance à la lumière de l'application du RGPD.

Téléchargement

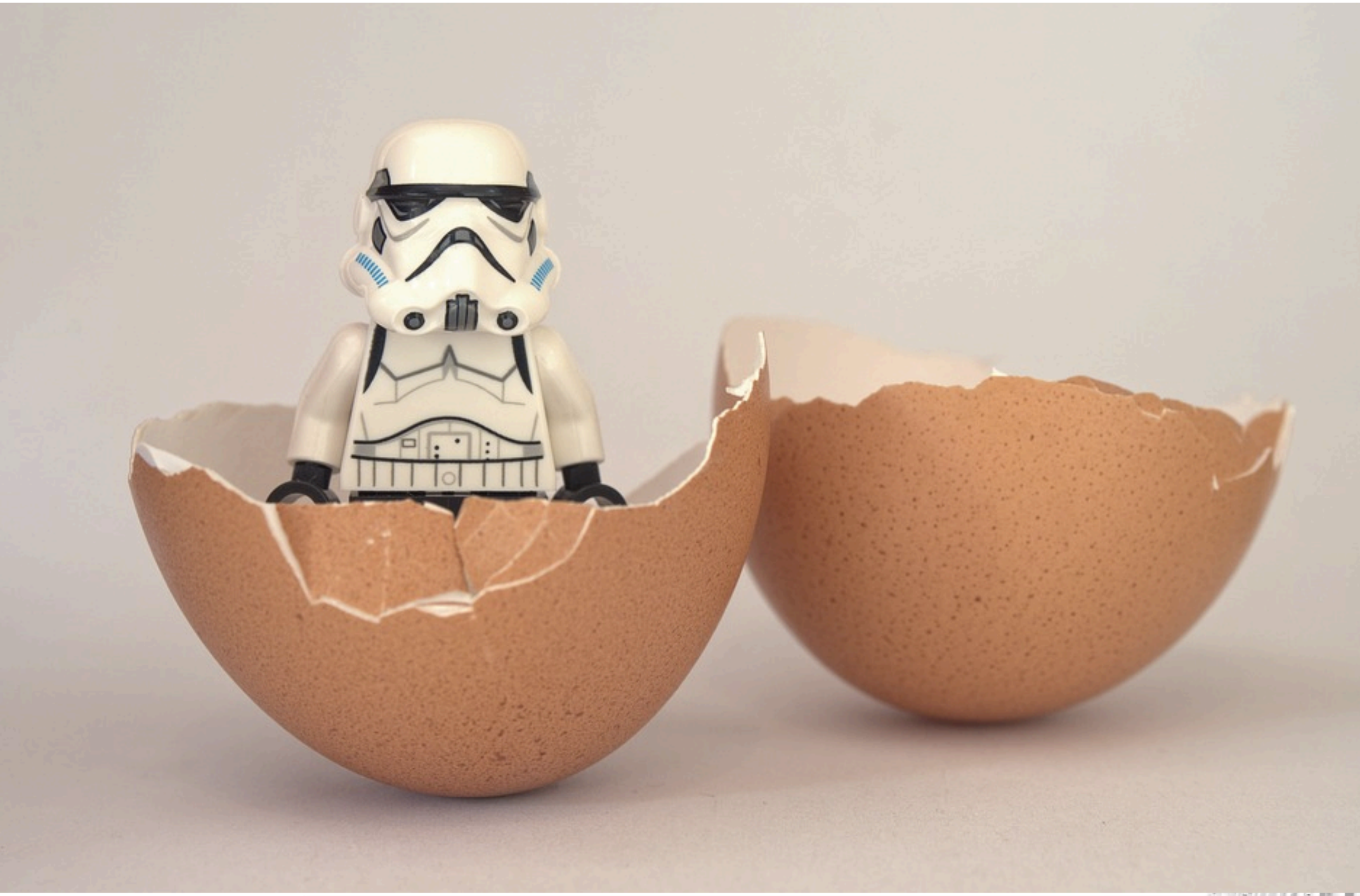
› Modèle de Registre des activités de traitement

La nascita di una nuova figura: il DPO

ARRAY

Avv. Giovanni Battista Gallus - Avv. Francesco Paolo Micozzi

La nascita di una nuova figura: il DPO

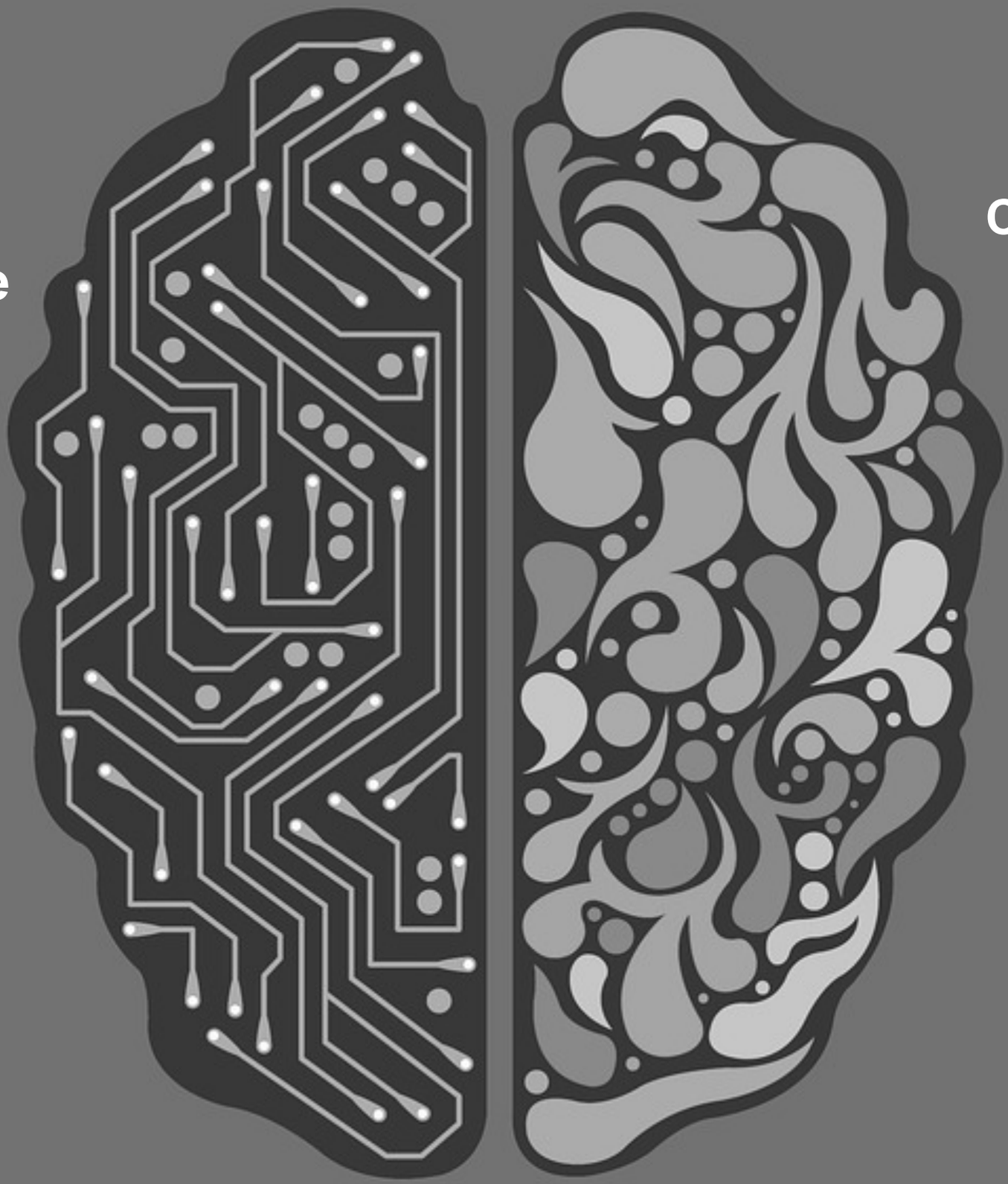


Art. 37, comma 5

5. 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**.

Una figura con differenti competenze

Tecniche / Informatiche



Comunicazione

Manageriali

Giuridiche

Art. 37, comma 5 - Requisiti del DPO

Qualità professionali del DPO

Conoscenza specialistica di norme su privacy e data protection

Capacità di assolvere ai compiti previsti dall'art. 39

II LIVELLO DI CONOSCENZA SPECIALISTICA:

A) deve persistere per tutta la durata di incarico di DPO;
B) non può essere valutato in astratto (cfr "bollino del DPO") ma deve essere valutato in concreto, ossia:
   a) deve essere adeguato al settore di attività del titolare o responsabile;
   b) **deve essere in grado di gestire la tipologia di dati trattati dal titolare o dal responsabile;**
   c) deve essere in grado di garantire il livello di sicurezza richiesto

Obbligatorietà della nomina del DPO

Soggetti Pubblici

“Autorità pubblica o organismo pubblico”

Articolo 37
Designazione del responsabile della protezione dei dati

1. Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:

a) il trattamento è effettuato da un'**autorità pubblica** o da un **organismo pubblico**, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

(97) Per i trattamenti effettuati da un'autorità pubblica, eccettuate le **autorità giurisdizionali** o **autorità giudiziarie indipendenti** quando esercitano le loro funzioni giurisdizionali,

Cosa si intende per “Autorità pubblica o organismo pubblico”

ARRAY Avv. Giovanni Battista Gallus - Avv. Francesco Paolo Micozzi

IN CONCLUSIONE...

Nel regolamento non si rinviene alcuna definizione di "autorità pubblica" o "organismo pubblico". **Il Gruppo di lavoro ritiene che tale definizione debba essere conforme al diritto nazionale;** conseguentemente, sono autorità pubbliche o organismi pubblici le autorità nazionali, regionali e locali ma, a seconda del diritto nazionale applicabile, la nozione ricomprende anche tutta una serie di altri organismi di diritto pubblico

Compiti del DPO

Compiti del DPO

1. offre consulenza a titolare, responsabile e dipendenti
2. fornisce il parere (se richiesto) sul DPIA
3. sorveglia sul rispetto della disciplina sulla protezione dati
4. coopera con l'Autorità di controllo
5. funge da punto di contatto per l'autorità di controllo
6. valuta i rischi che incombono sui dati personali trattati

In che modo si può valutare la capacità di assolvere a tali compiti?
(la valutazione è necessaria ai fini della individuazione del DPO)

Indipendenza e autonomia del DPO

ARRAY

Avv. Giovanni Battista Gallus - Avv. Francesco Paolo Micozzi

Art. 38, co. 3

Il titolare del trattamento e il responsabile del trattamento si assicurano che il DPO ***non riceva alcuna istruzione*** *per quanto riguarda l'esecuzione di tali compiti. ...*

Art. 38, co. 3

...

Il responsabile della protezione dei dati ***non è rimosso o penalizzato*** *dal titolare del trattamento o dal responsabile del trattamento* ***per l'adempimento dei propri compiti****.*

...

Indipendenza e autonomia

Art. 38, co. 3

...

Il responsabile della protezione dei dati ***riferisce direttamente al vertice gerarchico del titolare del trattamento*** *o* ***del responsabile*** *del trattamento.*

DPO e Trasparenza come accessibilità totale

DPO e Trasparenza come accessibilità totale

Quali interazioni?

Responsabile per la prevenzione della della corruzione e trasparenza

Amministrazione

Interessati

Data Protection officer

DPO e Trasparenza come accessibilità totale

Quali interazioni?

Data Protection officer

RPCT

Adempimento degli obblighi di pubblicazione

Pubblicazione di dati ulteriori anonimizzazione e riuso

Accesso generalizzato e dati personali

Data breach (violazione di dati personali)

DPO e accesso generalizzato

Data Protection officer

RPCT

Amministrazione

Valutazione della sussistenza di un pregiudizio concreto alla protezione dei dati personali ex art. 5bis D.lgs 33/2013

DPO e pubblicazioni

Data Protection officer

RPCT

Responsabili pubblicazione

Interessati

Data Protection By Default By Design

ARRAY

Avv. Giovanni Battista Gallus - Avv. Francesco Paolo Micozzi

Art. 5 - Principi applicabili al trattamento di dati personali

1. I dati personali sono

c) **adeguati, pertinenti e limitati** a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

2. Il titolare del trattamento è **competente per** il rispetto del paragrafo 1 e **in grado di comprovarlo** («responsabilizzazione»).

---

1. Personal data shall be

c) **adequate, relevant and limited** to what is necessary in relation to the purposes for which they are processed ('data minimisation');

2. The controller shall be **responsible for**, and be **able to demonstrate** compliance with, paragraph 1 ('accountability').

“Quello che non c’è non si rompe”

(*Henry Ford*)

La valutazione del rischio… quale rischio?

"I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale"

RISCHIO = PROBABILITÀ x DANNO MASSIMO IPOTIZZABILE

$$R = P \times D$$

Potenziali danni derivanti da trattamento di dati personali:

- **danno fisico**
- **danno materiale**
- **danno immateriale**

Natura dei dati e livello di rischio

Documentazione delle attività (Accountability)

Identificazione del rischio

Analisi e ponderazione del rischio

Predisposizione delle misure di contrasto dei rischi

Art. 25 GDPR

WHO? *il titolare del trattamento*

WHAT? *mette in atto* ***misure tecniche e organizzative adeguate****, (quali la pseudonimizzazione),*

WHEN? *sia* ***al momento di determinare i mezzi del trattamento*** *sia* ***all'atto del trattamento stesso***

HOW? *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 costituiti dal trattamento*

WHY? *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-Design / by-Default

Il GDPR non prevede un numero chiuso delle misure di prevenzione del rischio ma ne suggerisce, comunque, qualcuna:

- ridurre al minimo il trattamento dei dati personali;
- pseudonimizzare i dati personali il più presto possibile;
- offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali;
- consentire all'interessato di controllare il trattamento dei dati;
- consentire al titolare del trattamento di creare e migliorare caratteristiche di sicurezza.

Tali misure rientrano nel concetto di privacy-by-design e di privacy-by-default

Quando porsi il problema di privacy-by-default e by-design?

- ☑ In fase di **sviluppo** (produttori);
- ☑ In fase di **progettazione** (produttori);
- ☑ In fase di **selezione** (titolari e responsabili);
- ☑ In fase di **utilizzo** (titolari e responsabili),

di **applicazioni**, **servizi** e **prodotti** basati sul trattamento di dati personali o che trattano dati personali
(Considerando 78)

"*sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento*" (art. 25 GDPR)

Obblighi di sicurezza

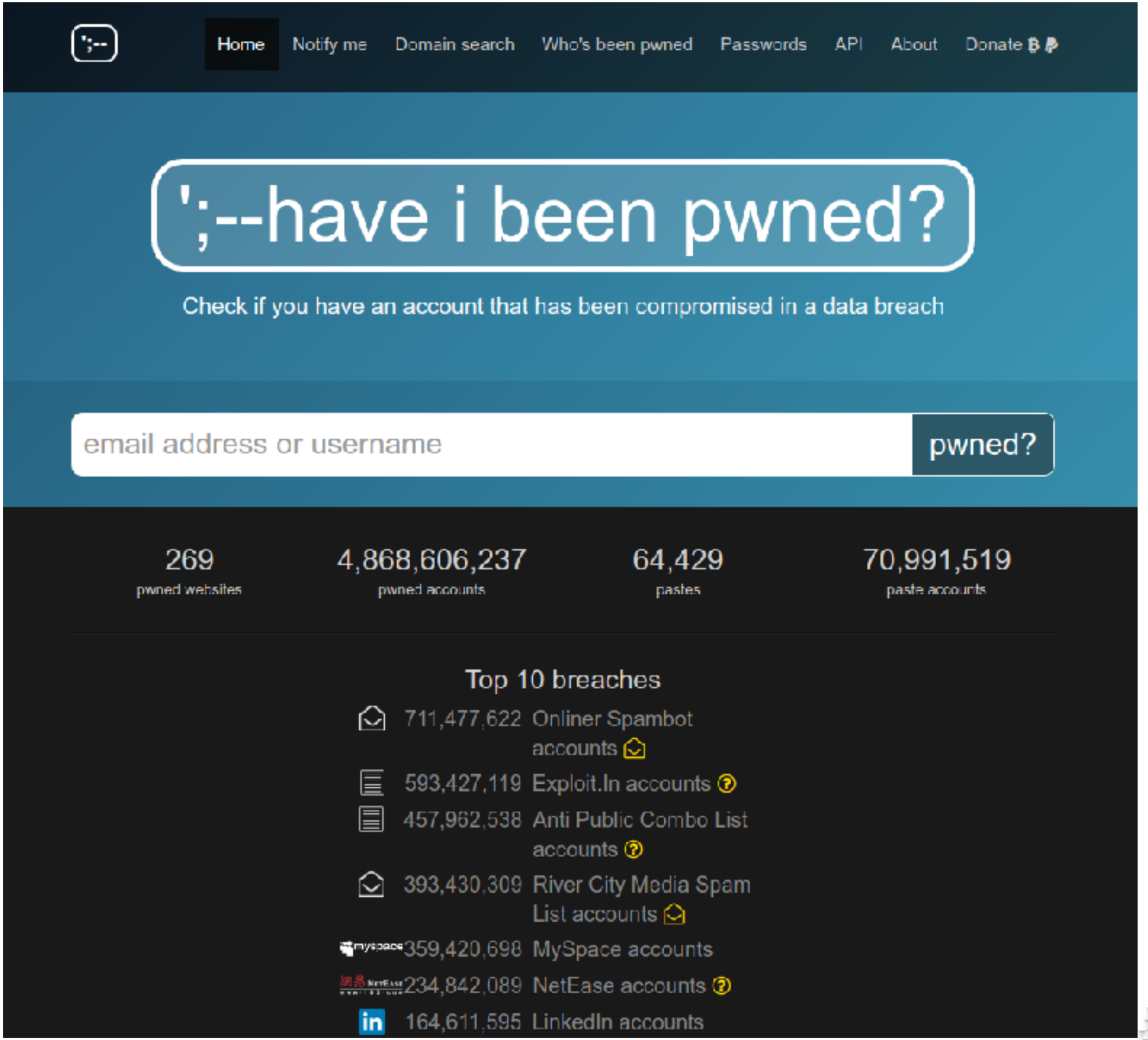
MISURE TECNICHE (no numero chiuso)

- **pseudonimizzazione** e **cifratura** dei dati personali (art. 32)
- capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità [**CIA**] (art. 32)
- capacità di assicurare su base permanente la **resilienza** dei sistemi e dei servizi di trattamento (art. 32)
- 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 al fine di garantire la sicurezza del trattamento (art. 32)
- Privacy-By-Default - minimizzazione (art. 25)
- Privacy-By-Design

MISURE ORGANIZZATIVE (no numero chiuso)

- Scelta corretta dei responsabili del trattamento - art. 28
- Formazione (di tutti i soggetti autorizzati al trattamento)
- Designazione dei rappresentanti dei titolari extra UE - art. 27
- Nomina del responsabile della protezione dei dati (DPO) - art. 37
- Redazione di policy specifiche (e eventuale integrazione con MOG e PTPCT)
- Eventuale adesione a codici di condotta
- Eventuale certificazione

Data Breach


Home
Notify me
Domain search
Who's been pwned
Passwords
API
About
Donate
';--have i been pwned?
Check if you have an account that has been compromised in a data breach
email address or username
pwned?
269
pwned websites
4,868,606,237
pwned accounts
64,429
pastes
70,991,519
paste accounts
Top 10 breaches
711,477,622 Onliner Spambot accounts
593,427,119 Exploit.In accounts
457,962,538 Anti Public Combo List accounts
393,430,309 River City Media Spam List accounts
359,420,698 MySpace accounts
234,842,089 NetEase accounts
164,611,595 LinkedIn accounts

Art. 33 GDPR

Notifica di una violazione dei dati personali all'autorità di controllo

1. In caso di violazione dei dati personali, il **titolare** del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, **entro 72 ore dal momento in cui ne è venuto a conoscenza**, a meno che sia improbabile che la violazione dei dati personali presenti un **rischio per i diritti e le libertà delle persone fisiche**.
Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è **corredata dei motivi del ritardo**.

Rischio per i diritti e le libertà delle persone fisiche

Valutazione caso per caso (WP29)

Art. 33 GDPR

Notifica di una violazione dei dati personali all'autorità di controllo
1. In caso di violazione dei dati personali, il **titolare** del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, **entro 72 ore dal momento in cui ne è venuto a conoscenza**, a meno che sia improbabile che la violazione dei dati personali presenti un **rischio per i diritti e le libertà delle persone fisiche**. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è **corredata dei motivi del ritardo**.

2. Il **responsabile del trattamento informa il titolare** del trattamento **senza ingiustificato ritardo** dopo essere venuto a conoscenza della violazione.

Questo ultimo obbligo va **specificato nell'accordo negoziale con il data processor**, ex art. 28, comma 3

[…] Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:
f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli **articoli da 32 a 36**, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

Art. 33 GDPR

3. La notifica di cui al paragrafo 1 deve almeno:
a) **descrivere** la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni **[records]** dei dati personali in questione;

Categorie di interessati:

utenti; persone con disabilità; soggetti vulnerabili; dipendenti etc

Categorie di dati:

health data, educational records, social care information, financial details, bank account numbers, passport numbers (WP29)

Art. 34 - Comunicazione all'interessato

1. 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 **senza ingiustificato ritardo**.
2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la **natura della violazione dei dati personali** e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).

b) comunicare **il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto** presso cui ottenere più informazioni;

c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Rischio improbabile – Nessuna "notificazione"

Assenza di rischio "elevato" - Nessuna "comunicazione"

Art. 34 - Comunicazione all'interessato

Modalità della comunicazione

- Messaggio specifico (no a inserimento in newsletter etc.)
- Comunicazione sul sito
- Eventuale pubblicazione su quotidiani e simili
- Attenzione al formato e alla lingua
- Attenzione ai phishing che simulano i data breach

Tempistica

è opportuno che tali modalità e procedure tengano conto dei legittimi interessi delle autorità incaricate dell'applicazione della legge **[law-enforcement authorities]**, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali. (C.88)

Valutazione di impatto (DPIA)

Verifica preliminare

Notificazione

Accountability

Valutazione d'impatto

Una valutazione d'impatto sulla protezione dei dati è un **processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi** per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali

[Art. 29 WP, Linee Guida]

Processo complessivo di identificazione, analisi, valutazione, consultazione, comunicazione e pianificazione del trattamento dì potenziali impatti sulla privacy nel trattamento di dati personali, contestualizzata all'interno del quadro dì riferimento aziendale complessivo per la gestione del rischio.

[ISO/IEC 29134]

Valutazione d'impatto

non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento ma soltanto quando il trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche"

[Art. 29 WP, Linee Guida]

Approccio basato sul rischio

Who	Controller (+ DPO)
What	Valutazione d'impatto
Where	Imprese e PA
When	Probabilità di un alto rischio
Why	Trattare il rischio
How	Procedure, standard, audit

Art. 35 GDPR (ipotesi generale)

1. 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.

“Likely to result in a high risk”
La “Regola del Due”

1. Valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di "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. processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente
3. monitoraggio sistematico
4. dati sensibili o dati aventi carattere altamente personale:
5. trattamento di dati su larga scala
6. creazione di corrispondenze o combinazione di insiemi di dati, ad esempio a partire da dati derivanti da due o più operazioni di trattamento svolte per finalità diverse e/o da titolari del trattamento diversi secondo una modalità che va oltre le ragionevoli aspettative dell'interessato
7. dati relativi a interessati vulnerabili (es. minori)
8. uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative
9. quando il trattamento in sé "impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto”

Art. 35 GDPR (ipotesi tipizzate)

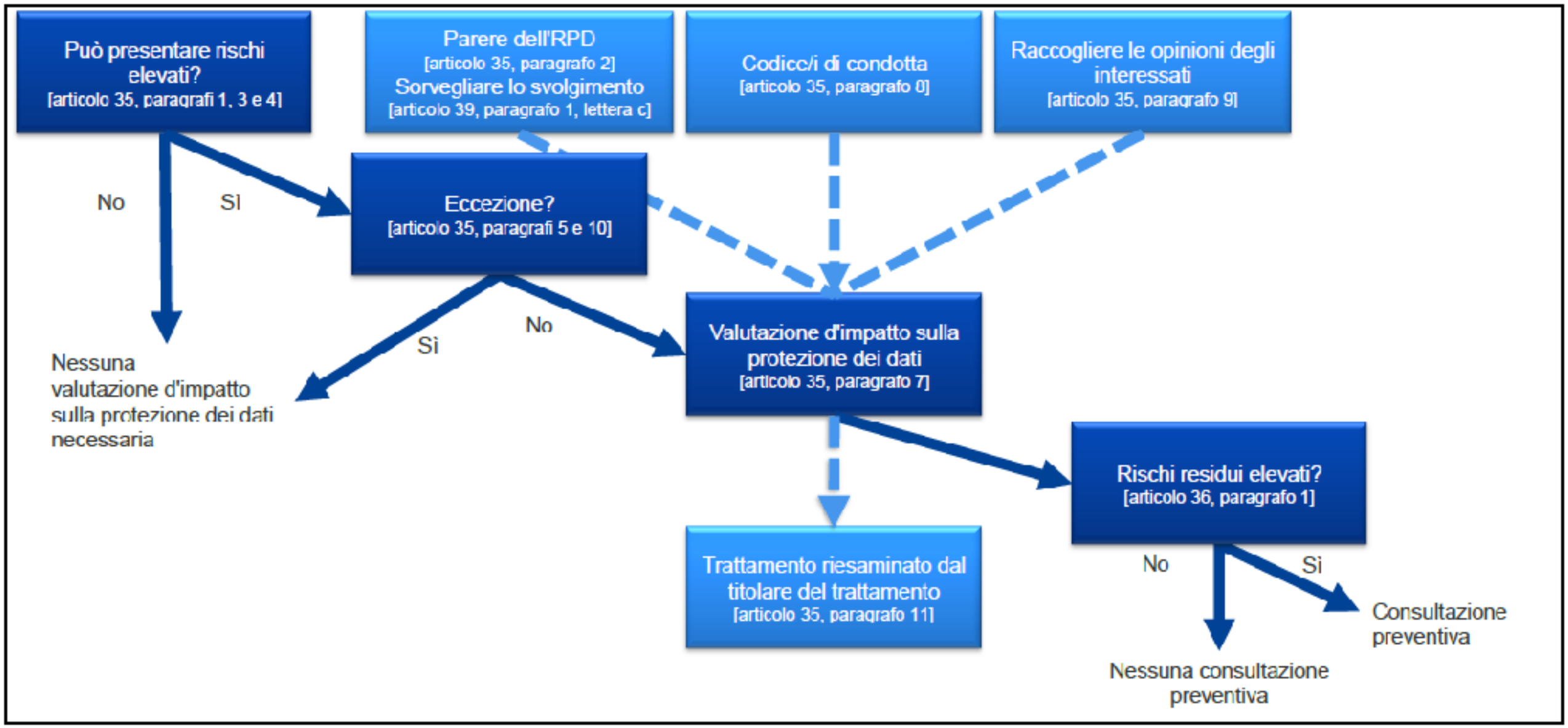
3. La **valutazione d'impatto** sulla protezione dei dati di cui al paragrafo 1 **è richiesta** in particolare **nei casi seguenti**:

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; o

c) la **sorveglianza sistematica su larga scala** di una zona accessibile al pubblico.

Lo schema dell'art. 29 WP



Le responsabilità e le sanzioni

ARRAY

Avv. Giovanni Battista Gallus - Avv. Francesco Paolo Micozzi

Responsabilità e sanzioni nel GDPR

Art. 83 - condizioni generali sulle sanzioni amministrative pecuniarie

Art. 84 - delega agli Stati membri all'adozione di sanzioni per violazioni non previste dal GDPR

L'art. 83 - Se e in quale misura sanzionare le PA

7. Fatti salvi i poteri correttivi delle autorità di controllo a norma dell'articolo 58, paragrafo 2, ***ogni Stato membro può prevedere norme che dispongano se e in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici*** *istituiti in tale Stato membro.*

Comitato europeo per la protezione dei dati

ai sensi dell'articolo 70, paragrafo 1, lettera e), il comitato europeo per la protezione dei dati ha la facoltà di pubblicare linee guida, raccomandazioni e migliori prassi al fine di promuovere l'applicazione coerente del regolamento, e l'articolo 70, paragrafo 1, lettera k), specifica che è prevista l'elaborazione di linee guida riguardanti la previsione di sanzioni amministrative pecuniarie

I poteri delle DPA

Le disposizioni di cui all'articolo 58, paragrafo 2, lettere da b) a j), indicano gli strumenti che le autorità di controllo hanno a disposizione per far fronte a un'inadempienza da parte di un titolare del trattamento o responsabile del trattamento:

(B)rivolgere **ammonimenti** al titolare o al responsabile del trattamento
(C)ingiungere al titolare o al responsabile del trattamento di **soddisfare le richieste dell'interessato**;
(D)ingiungere al titolare del trattamento o al responsabile del trattamento di **conformare i trattamenti alle disposizioni del regolamento**, se del caso, in una determinata maniera ed entro un determinato termine;
(E)ingiungere al titolare del trattamento di **comunicare all'interessato una violazione dei dati personali**;
(F)**imporre una limitazione provvisoria o definitiva al trattamento**;
(G)**ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento**;
(H)**revocare la certificazione**;
(I)**infliggere una sanzione amministrativa pecuniaria**;
(J)**ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo** o un'organizzazione internazionale.

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI

17/IT

WP 253

Linee guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del regolamento (UE) n. 2016/679

Adottate il 3 ottobre 2017

Sanzioni “multilivello”

Le sanzioni amministrative pecuniarie possono essere inflitte in combinazione o in sostituzione delle misure previste dall’art. 58 GDPR

Principi destinati alle DPA (in Italia il Garante)

1. La violazione del regolamento dovrebbe comportare l'imposizione di "**sanzioni equivalenti**"

2. Come tutte le misure correttive scelte dalle autorità di controllo, le sanzioni amministrative pecuniarie dovrebbero essere "**effettive, proporzionate e dissuasive**"

3. L'autorità di controllo competente effettuerà una valutazione "in ogni singolo caso"

4. Un approccio armonizzato alle sanzioni amministrative pecuniarie in materia di protezione dei dati richiede la partecipazione attiva delle autorità di controllo e lo scambio di informazioni tra le stesse

L'art. 83 - concorso di violazioni

3. Se, in relazione allo stesso trattamento o a trattamenti collegati, un titolare del trattamento o un responsabile del trattamento viola, con dolo o colpa, varie disposizioni del presente regolamento, ***l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave.***

L’art. 83 - importo delle sanzioni

4. In conformità del paragrafo 2, ***la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 10.000.000 EUR****, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:*

a) gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43;

b) gli obblighi dell'organismo di certificazione a norma degli articoli 42 e 43;

c) gli obblighi dell'organismo di controllo a norma dell'articolo 41, paragrafo 4;

L'art. 83 - importo delle sanzioni

5. In conformità del paragrafo 2, ***la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 20.000.000 EUR****, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:*

a) i principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9;

b) i diritti degli interessati a norma degli articoli da 12 a 22;

c) i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49;

d) qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX;

e) l'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 ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1.

Art 77 Diritto di proporre reclamo all'autorità di controllo

1. 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 ove si è verificata la presunta violazione.*

Art 78 Diritto a un ricorso giurisdizionale effettivo nei confronti dell'autorità di controllo

1. Fatto salvo ogni altro ricorso amministrativo o extragiudiziale, ogni persona fisica o giuridica ha il diritto di proporre un ricorso giurisdizionale effettivo avverso una decisione giuridicamente vincolante dell'autorità di controllo che la riguarda.

2. Fatto salvo ogni altro ricorso amministrativo o extragiudiziale, ciascun interessato ha il diritto di proporre un ricorso giurisdizionale effettivo qualora l'autorità di controllo che sia competente ai sensi degli articoli 55 e 56 non tratti un reclamo o non lo informi entro tre mesi dello stato o dell'esito del reclamo proposto ai sensi dell'articolo 77.

Art 79 Diritto a un ricorso giurisdizionale effettivo nei confronti del titolare del trattamento o del responsabile del trattamento

1. Fatto salvo ogni altro ricorso amministrativo o extragiudiziale disponibile, compreso il diritto di proporre reclamo a un'autorità di controllo ai sensi dell'articolo 77, ogni interessato ha il diritto di proporre un ricorso giurisdizionale effettivo qualora ritenga che i diritti di cui gode a norma del presente regolamento siano stati violati a seguito di un trattamento.

2. Le azioni nei confronti del titolare del trattamento o del responsabile del trattamento sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui il titolare del trattamento o il responsabile del trattamento ha uno stabilimento. In alternativa, tali azioni possono essere promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'interessato risiede abitualmente, salvo che il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica di uno Stato membro nell'esercizio dei pubblici poteri.

Art 82 Diritto al risarcimento e responsabilità

1. 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.

2. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.

3. ***Il titolare*** *del trattamento* ***o il responsabile*** *del trattamento* ***è esonerato dalla responsabilità****, a norma del paragrafo 2* ***se dimostra che l'evento dannoso non gli è in alcun modo imputabile****.*

Roadmap GDPR

ARRAY

Avv. Giovanni Battista Gallus - Avv. Francesco Paolo Micozzi

Considerando 171

Il presente regolamento dovrebbe abrogare la direttiva 95/46/CE. Il trattamento già in corso alla data di applicazione del presente regolamento dovrebbe essere reso conforme al presente regolamento **entro un periodo di due anni** dall'entrata in vigore del presente regolamento. Qualora il trattamento si basi sul consenso a norma della direttiva 95/46/CE, non occorre che l'interessato presti nuovamente il suo consenso, se questo è stato espresso secondo modalità conformi alle condizioni del presente regolamento, affinché il titolare del trattamento possa proseguire il trattamento in questione dopo la data di applicazione del presente regolamento.

Le decisioni della Commissione e le autorizzazioni delle autorità di controllo basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite o abrogate.

10 steps towards GDPR

1. Analisi del contesto interno sui dati personali
2. Individuazione dell'organigramma
3. Verifica delle policy e degli altri documenti
4. Creazione del Registro dei Trattamenti
5. Verifica delle misure tecniche impiegate per ciascun trattamento
6. Mettere in atto il sistema di segnalazione di data breach
7. Eseguire la DPIA (ove richiesto)
8. Analisi della base normativa/contrattuale per ciascun trattamento
9. Individuazione e nomina del DPO
10. Verificare ipotesi di trattamenti transfrontalieri

Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now

1 Awareness

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2 Information you hold

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3 Communicating privacy information

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4 Individuals' rights

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5 Subject access requests

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6 Lawful basis for processing personal data

You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

7 Consent

You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

8 Children

You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

9 Data breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10 Data Protection by Design and Data Protection Impact Assessments

You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.

11 Data Protection Officers

You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.

12 International

If your organisation operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

ico.
Information Commissioner's Office

ico.org.uk

Grazie

per l'attenzione

ARRAY

Avv. Giovanni Battista Gallus - Avv. Francesco Paolo Micozzi