GENERAL SERVICE lab

Formazione - Sicurezza - Compliance

IL NUOVO REGOLAMENTO GENERALE UE SULLA PROTEZIONE DEI DATI PERSONALI N. 679/2016

Analisi pratica del quadro generale di insieme e dei nuovi adempimenti privacy.

Assioma Group S.r.l.

GENERAL SERVICE SOC. COOP.

SICUREZZA - SALUTE - QUALITA' - AMBIENTE - FORMAZIONE

GENERAL SERVICE lab

Formazione - Sicurezza - Compliance

Assioma Group S.r.l.

STUDIO LEGALE PALMA
lawers & consultans
avv. Francesco Palma

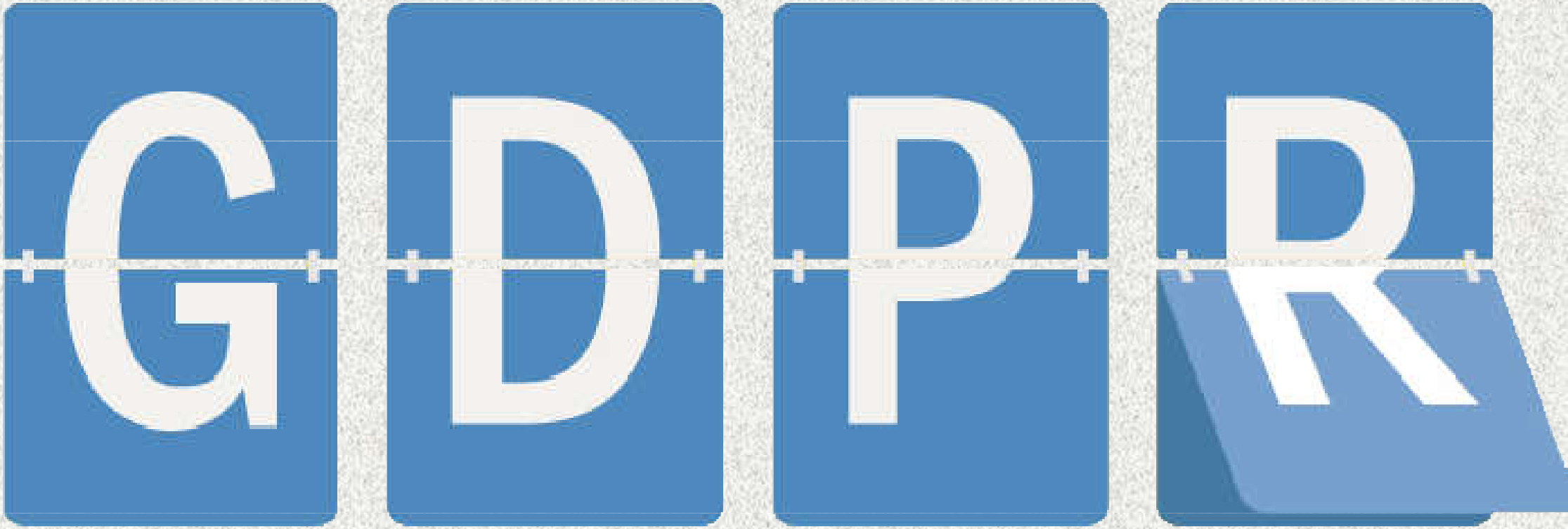
GENERAL SERVICE SOC. COOP.
SICUREZZA - SALUTE - QUALITA' - AMBIENTE - FORMAZIONE

CHI SIAMO E COSA FACCIAMO

PRIVACY
ANTIRICICLAGGIO
FORMAZIONE
SICUREZZA SUL LAVORO
HACCP

COMPLIANCE
SUPPLY CHAIN
LEAN MANAGEMENT
FORMAZIONE MANAGERIALE
GESTIONE CRISI D'IMPRESA

Il Regolamento per la Protezione dei Dati Personali



A seguito della pubblicazione sulla Gazzetta Ufficiale dell'Unione Europea del 04 Maggio 2016, è entrato formalmente in vigore il 24 maggio 2016 il Regolamento Europeo per la Protezione dei Dati Personali 2016/679 o nella sua accezione inglese **General Data Protection Regulation (GDPR).**

Data di entrata in vigore

24 Maggio 2016

Data di applicazione

25 Maggio 2018

ENTRATA IN VIGORE E APPLICABILITA'

ENTRATA IN VIGORE

✓Pubblicazione nella Gazzetta Ufficiale dell'Unione Europea n. 119/2016: **4 Maggio 2016**.

✓Entrata in vigore: **25 Maggio 2016**.

✓Tutti i soggetti interessati hanno **due anni di tempo** per adeguare alle nuove norme le politiche del trattamento dei dati.

✓Applicabilità in tutti i Paesi della UE: **25 Maggio 2018**.

✓Il Regolamento sarà **immediatamente applicabile** senza necessità di recepimento.

Legge di delegazione europea 2016-2017

25 OTTOBRE 2017 n° 163

(Entrata in vigore del provvedimento: 21/11/2017)

Articolo 13

✓(Delega al Governo per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE)

Articolo 13

✓Il comma 1 dell'articolo reca delega al Governo ad adottare, entro sei mesi dalla data di entrata in vigore della presente legge, con le procedure di cui all'articolo 31 della legge 24 dicembre 2012, n. 234, previo parere delle competenti Commissioni parlamentari e del Garante per la protezione dei dati personali, uno o più decreti legislativi al fine di adeguare il quadro normativo nazionale alle disposizioni del regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE

Il **comma 3 individua i seguenti principi e criteri direttivi (oltre quelli generali già previsti dall'articolo 32 della legge n. 234 del 2012) ai quali l'Esecutivo deve attenersi nell'esercizio della delega:**

- abrogare espressamente le disposizioni del Codice in materia di trattamento dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196 e successive modificazioni (Codice della *privacy*) ***incompatibili*** *con le disposizioni contenute nel regolamento (UE) n. 2016/679;*
- **modificare** il Codice della *privacy limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel regolamento (UE) n. 2016/679;*

Il Governo approva in esame preliminare il decreto di adeguamento del Codice della Privacy

Nella seduta del 21 Marzo 2017, il Consiglio dei Ministri ha trattato il tema dell'armonizzazione della normativa italiana rispetto alle disposizioni del Regolamento UE 2016/679, chiarendo quale sarà il futuro dell'attuale Codice della Privacy.

Il Consiglio dei Ministri, su proposta del Presidente **Paolo Gentiloni** e del **Ministro della giustizia Andrea Orlando**, ha approvato, in esame preliminare, un decreto legislativo che, in attuazione dell'art. 13 della legge di delegazione europea 2016-2017 (legge 25 ottobre 2017, n. 163), introduce disposizioni per l'adeguamento della normativa nazionale alle disposizioni del **Regolamento europeo** relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Il Governo approva in esame preliminare il decreto di adeguamento del Codice della Privacy

A far data dal 25 maggio 2018, data in cui le disposizioni di diritto europeo acquisteranno efficacia, il vigente Codice in materia di protezione dei dati personali, di cui al **decreto legislativo 30 giugno 2003, n. 196, sarà abrogato** e la nuova disciplina in materia sarà rappresentata principalmente dalle disposizioni del suddetto Regolamento, immediatamente applicabili, e da quelle recate dallo schema di decreto volte ad armonizzare l'ordinamento interno al nuovo quadro normativo dell'Unione Europea in tema di tutela della privacy. Il nuovo decreto sostituirà l'attuale Codice della Privacy e che entrerà in vigore al momento dell'abrogazione del D.Lgs. 196/2003.

Fonte: *Governo Italiano Presidenza del Consiglio dei Ministri*

Alcuni primi dettagli del GDPR

Per favorire l'applicazione del GDPR ciascuno stato membro è stato chiamato ad istituire un'**Autorità Sovrintendente Indipendente** per

- ✓ dare udienza ai reclami,
- ✓ effettuare indagini,
- ✓ sanzionare le infrazioni amministrative,
- ✓ ecc.

- Le autorità sovrintendenti in ciascuno stato membro collaboreranno con le altre, fornendo assistenza reciproca e organizzando operazioni congiunte sotto il coordinamento e la supervisione di una apposita commissione europea per la protezione dei dati (EDPB, European Data Protection Board).

Il WP 29

- Inizialmente il gruppo di lavoro delle diverse autorità è stato citato anche come **WP 29 (Working Party Article 29)** poiché è stato istituito dall'art. 29 della direttiva 95/46, come organismo consultivo e indipendente. (Organismo che riunisce tutti i Garanti Privacy europei)

- Il WP 29 è composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro, dal GEPD (Garante europeo della protezione dei dati), nonché da un rappresentante della Commissione appositamente istituita in sede UE.

- Il 25 Maggio 2018, all'atto della piena applicazione del GDPR, il WP29 verrà sostituito dall'EDPB (European Data Protection Board)

Compiti del WP 29

Fra i compiti più rilevanti del WP29 vi sono i seguenti:

- **formulare pareri** sul livello di tutela nella Comunità e nei paesi terzi
- **fornire consulenze** alla Commissione in merito ad ogni progetto di modifica della direttiva, ogni progetto di misure addizionali o specifiche da prendere ai fini della tutela dei diritti e delle libertà, nonché in merito a qualsiasi altro progetto di misure comunitarie che incidano su tali diritti e libertà
- **formulare pareri** sui codici di condotta elaborati a livello comunitario
- **formulare** di propria iniziativa **raccomandazioni** su qualsiasi questione riguardi la protezione dei dati personali nella Comunità
- **definire i criteri** di adeguatezza per i paesi terzi.

Meccanismo di coerenza all'interno dell'UE

Il Regolamento prevede un **MECCANISMO DI COERENZA**, gestito dal Garante Europeo per la Protezione dei Dati (GEPD, oppure nella versione inglese EDPS, European Data Protection Supervisor) che uniforma l'interpretazione e applicazione del Regolamento in tutti i Paesi dell'Unione.

In particolare viene indicato che, **qualora ci siano delle divergenze** tra le legislazioni degli stati membri che possano pregiudicare l'equivalenza della tutela delle persone, **interviene il WP29** informando la speciale commissione dell'UE, formulando pareri e raccomandazioni.

La Commissione è tenuta ad informare il gruppo del seguito dato ai suoi pareri e raccomandazioni.

14

Il riconoscimento di una Leading Authority favorisce la disponibilità di un punto di contatto unico

- Qualora un'impresa abbia più stabilimenti nell'UE, avrà un'unica Autorità sovrintendente come propria «Autorità principale« a cui fare riferimento, sulla base dell'ubicazione del proprio "**stabilimento principale**" (ossia il luogo dove si realizzano le principali attività di gestione).

- L'Autorità principale agirà quale "**sportello unico** (noto anche come meccanismo dell'**One Stop Shop**, ovvero unico negozio dove trovo tutto)" per supervisionare tutte le attività di gestione dati di quell'impresa nell'UE.

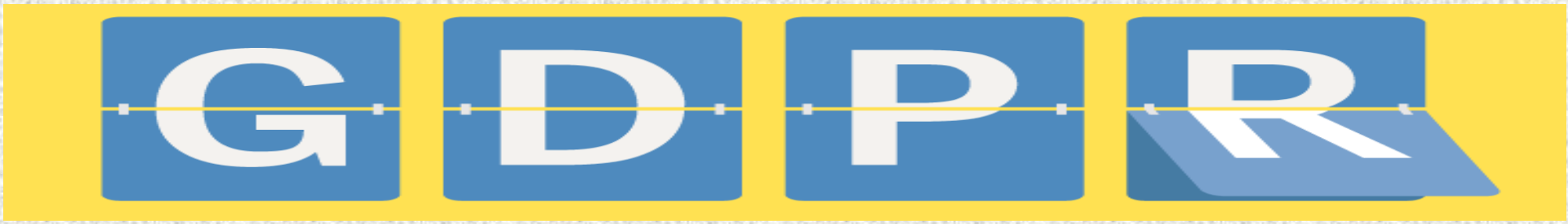
L'**Autorità principale fungerà anche da capofila** (**Leading Authority**) nei confronti delle altre Autorità nazionali cooperando ed avendo la competenza di emettere decisioni vincolanti per la altre autorità.

PRINCIPALI MODIFCHE INTRODOTTE DAL REGOLAMENTO

Il Regolamento Generale per la Protezione dei Dati Personali si compone di 11 Capi suddivisi in 99 Articoli e 173 Considerando

SCHEMA RIEPILOGATIVO

LE MODIFICHE	LE NOVITA'
✓ Modifica di definizioni esistenti	▪ Estensione ambito territoriale
✓Specificazione dei ruoli e compiti di Titolare e Responsabile	▪Nuove definizioni (profilazione, dati biometrici, ecc.)
✓ Informativa rafforzata	▪Il Responsabile della protezione dei dati (c.d. "Data Protection Officer")
✓ Il consenso	▪ Il Registro dei trattamenti
✓ Specificazione di diritti	▪ La valutazione preventiva d'impatto
✓ Inasprimento sanzioni	▪ Notifica dei data breach
	▪ Privacy *by design* – privacy *by default*
	▪ Diritto all'oblio e a Portabilità dei dati



Tra i principi introdotti dal regolamento, una grande novità è costituita dal principio della "**responsabilizzazione**" (*accountability nell'accezione inglese*) dei titolari, ossia, dall'adozione di comportamenti proattivi volti a dimostrare la concreta adozione di misure necessarie ad assicurare l'applicazione del regolamento. In altri termini, viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei **dati personali** all'interno della propria azienda.

Le aziende si trovano pertanto nella condizione di dover soddisfare nuove esigenze:

Privacy by Design

Privacy by Default

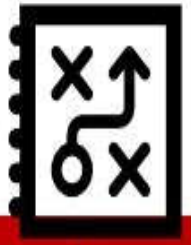
Privacy by Design

Privacy by design significa che ogni nuovo servizio o processo aziendale che utilizza i dati personali deve prendere in considerazione la protezione di quei dati. Le aziende devono essere in grado di dimostrare che hanno adottato un adeguato grado di sicurezza e che monitorano la compliance. In pratica, questo significa che la protezione dei dati deve essere un aspetto determinante lungo l'intero ciclo di sviluppo di un nuovo sistema.

:

Privacy by Default

Privacy by default significa semplicemente che quando un cliente acquista un nuovo prodotto o servizio vengono applicate automaticamente le impostazioni di privacy più rigorose. In altri termini, non dovrebbero essere necessarie modifiche manuali alle impostazioni sulla privacy da parte dell'utente. I titolari o responsabili del trattamento potranno archiviare dati solo per il tempo strettamente necessario a fornire un prodotto o servizio.



Applicare

CONFORMITÀ

Adeguarsi alle normative

+

Dimostrare

RESPONSABILIZZAZIONE

Dimostrare di adeguarsi alle normative

+

Manutenere

GESTIONE

Proteggere i dati e monitorare il livello di protezione

AMBITO DI APPLICABILITÀ MATERIALE

✓Si applica solo al trattamento dei dati personali di **persone fisiche;**

✓Riguarda trattamenti interamente o parzialmente **automatizzati o non automatizzati,** se i dati personali sono contenuti in un **archivio** o sono destinati a confluirvi;

✓Il Regolamento non si applica ai trattamenti di dati personali effettuati:

a)da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;

b) da autorità di pubblica sicurezza;

c)per attività che non rientrano nell'ambito di applicazione del diritto dell'UE.

AMBITO DI APPLICABILITÀ TERRITORIALE

Il Regolamento si applica:

1) al trattamento di dati personali effettuato da un **Titolare o Responsabile stabilito nella UE,** indipendentemente dal fatto che il trattamento sia effettuato o meno nella UE;

2) al trattamento di dati personali effettuato da **Titolari o Responsabili non stabiliti nell'UE,** indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione, se il **trattamento ha ad oggetto dati personali di interessati che si trovano nella UE** e riguarda (i) **l'offerta di beni o servizi** (anche non a pagamento) ai suddetti interessati oppure
(ii) il **monitoraggio** del loro comportamento nel territorio della UE;

3) al trattamento effettuato da un Titolare stabilito in uno **Stato extra UE soggetto al diritto di uno Stato UE** in virtù del diritto internazionale pubblico.

25

GENERAL SERVICE lab

Formazione - Sicurezza - Compliance

Le nuove definizioni

PRINCIPALI NUOVE DEFINIZIONI

✓Eliminata la definizione di dati **sensibili** e di **dati giudiziari;**

✓Ora si parla di "**Categorie particolari di dati personali":** dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale o a partiti politici, i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;

✓**Dati relativi alla salute:** 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;

PRINCIPALI NUOVE DEFINIZIONI

✓**Dati genetici**: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

✓**Dati biometrici**: 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

PRINCIPALI NUOVE DEFINIZIONI

- **Consenso dell'interessato:** qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

✓ **Pseudonimizzazione:** il trattamento di dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

LA PROFILAZIONE

✓Introdotta per la prima volta **una definizione e una regolamentazione del particolare trattamento rappresentato dalla profilazione dell'interessato**, giuridicamente definita come "*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*".

✓In linea generale è vietata ("*L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona*") a meno che non vi siano circostanze specifiche, tra le quali il **chiaro consenso informato dell'interessato**.

✓I trattamenti di profilazione rappresentano poi uno dei presupposti che **rendono obbligatoria la valutazione preventiva** di impatto sulla protezione dei dati.

PRINCIPALI DEFINIZIONI MODIFICATE

✓**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 caratteristicche della sua identità fisica fisiologica genetica psichica, economica, culturale o sociale.

✓**Trattamento:** 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

PRINCIPALI DEFINIZIONI MODIFICATE

✓**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;

✓**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;

✓**Terzo**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile

32

GENERAL SERVICE lab

Formazione - Sicurezza - Compliance

Nuovi obblighi nei rapporti tra i soggetti

NUOVI OBBLIGHI NEI RAPPORTI TRA SOGGETTI

il Regolamento introduce **degli obblighi organizzativi nuovi** con riferimento ai loro ruoli e funzioni, come ad esempio i seguenti:

✓il Titolare deve attuare **misure tecniche ed organizzative adeguate per garantire e dimostrare che il trattamento è effettuato conformemente al Regolamento**. Le misure devono essere riesaminate periodicamente e aggiornate, ove necessario. L'adesione a Codici di condotta o a meccanismi di certificazione, può essere utilizzata come elemento per dimostrare il rispetto degli obblighi imposti al Titolare del trattamento;

✓In caso di **contitolarità del trattamento:** i Contitolari devono stipulare tra loro **uno specifico accordo interno** che disciplini in modo trasparente le rispettive responsabilità e rifletta adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo va messo a disposizione dell'interessato;

IL CONTITOLARE DEL TRATTAMENTO

REGOLAMENTO 2016/679: articoli art. 4 (comma 7) , 26, 82
Considerando 79, 146;

Il Regolamento prevede anche l'ipotesi che per il medesimo trattamento di dati sia possibile individuare più titolari del trattamento.
È, infatti, possibile che due (o più) soggetti si trovino contemporaneamente, ciascuno per la propria area di competenza, ad essere e agire come titolari del trattamento (si veda anche Gruppo di lavoro articolo 29, Parere 1/2010 - WP 169).
Si ha in questo caso una situazione di **CONTITOLARITÀ**

IL CONTITOLARE DEL TRATTAMENTO

DEFINIZIONE DI UN RAPPORTO DI CO-TITOLARITA'

Qualora due o più Titolari (Controller) determinano congiuntamente le finalità e gli strumenti del trattamento di dati personali, gli stessi sono corresponsabili.

I Contitolari devono, per mezzo di un contratto scritto, decidere se e come ripartire le responsabilità rispetto agli obblighi relativi al Reg 679/2016 (ad esempio, un contitolare si assume la responsabilità di fornire informazioni chiare agli interessati, mentre l'altro contitolare si assume il compito di garantire la sicurezza dei dati).

Una sintesi del contratto tra i contitolari deve essere messo a disposizione delle persone interessate. il contratto può designare un unico punto di contatto per gli interessati.

IL CONTITOLARE DEL TRATTAMENTO

DEFINIZIONE DI UN RAPPORTO DI CO-TITOLARITA'

In molti casi (in particolare quando il trattamento avviene nell'ambito di un gruppo di imprese), i diversi soggetti possono non essere consapevole di trovarsi in una situazione di contitolarità. Il Regolamento chiede che diversi soggetti che trattano i dati valutino le possibili situazioni di contitolarità e , ove ne emergano, stipulino i necessari contratti.

Le persone interessate hanno il diritto di far valere i propri diritti contro uno qualsiasi dei soggetti che assumono la qualifica di contitolare.
In particolare, ogni contitolare è responsabile in toto per il danno causato: più esattamente il Regolamento introduce per i contitolari un principio di solidarietà, non presente nella Direttiva precedente.

NUOVI OBBLIGHI NEI RAPPORTI TRA SOGGETTI

- ✓ **Obbligatoria** per il Titolare la **nomina del Responsabile del trattamento, anche esterno (Outsourcer),** va documentata con un "*contratto o altro atto giuridico*", stipulato in forma scritta anche su supporto elettronico, che regoli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento. Ammessa la designazione di Sub-Responsabili previa autorizzazione scritta, specifica o generale del Titolare del trattamento;

- ✓ **Incaricati del trattamento (Processor)**: categoria di soggetti, identificata con le ***"persone autorizzate al trattamento"*** non è definita formalmente, ma disciplinata indirettamente. Viene previsto per il Titolare l'obbligo di indicare le persone autorizzate all'interno della sua struttura;

GENERAL SERVICE lab

Formazione - Sicurezza - Compliance

La nuova figura del *Data Protection Officer*

Il Responsabile della protezione dei dati

(Data Protection Officer)

La designazione del DPO è **obbligatoria** (da parte del Titolare o del Responsabile del trattamento) **solo se**:

1.il trattamento **è effettuato da un'autorità pubblica o da un organismo pubblico**, eccettuate le autorità giurisdizionali.

Il Responsabile della protezione dei dati

(Data Protection Officer)

Il WP 29 ritiene che tale definizione debba essere interpretata conformemente a (ciascun) diritto nazionale. E tuttavia, è bene evidenziare che nelle Linee guida del 13 dicembre 2016 viene "raccomandata" la nomina del DPO anche per quegli "**organismi privati incaricati di funzioni pubbliche o che esercitano pubblici poteri.**

Il Responsabile della protezione dei dati

(Data Protection Officer)

2. le attività **principali** del Titolare del trattamento o del Responsabile del trattamento consistono in **trattamenti che,** per natura, ambito di applicazione e/o finalità, **richiedono il monitoraggio regolare e sistematico degli interessati su larga scala**;

3. le attività **principali** del Titolare del trattamento o del Responsabile del trattamento consistono nel trattamento, **su larga scala**, di categorie particolari di dati di cui all'art. 9 o 10 del Regolamento (dati che rivelino l'origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, dati genetici, biometrici, dati relativi alla salute o alla vita sessuale o orientamento sessuale, o dati relativi a condanne penali e reati). . (escluse comunque le autorità giurisdizionali)

TRATTAMENTI SU LARGA SCALA

Il considerando 91 fornisce indicazioni in proposito, ricomprendendovi, in particolare, "**trattamenti… che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato**".

lo stesso "considerando 91" prevede in modo specifico che "Il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato".

TRATTAMENTI SU LARGA SCALA

Il Working Party 29 raccomanda di tenere conto, in particolare, dei seguenti fattori:

A. - il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;

B. - il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;

C. - la durata, ovvero la persistenza, dell'attività di trattamento;

D. - la portata geografica dell'attività di trattamento

MONITORAGGIO REGOLARE E SISTEMATICO DEGLI INTERESSATI

Secondo Il considerando 24, vi rientra certamente ogni forma di tracciamento e profilazione su Internet anche per finalità di pubblicità comportamentale.

Le linee guida evidenziano tuttavia che la nozione di monitoraggio non trova applicazione solo con riguardo all'ambiente online.

MONITORAGGIO REGOLARE E SISTEMATICO DEGLI INTERESSATI

L'aggettivo "**regolare**" ha almeno uno dei seguenti significati a giudizio del Working Party:

A. che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito;
B. ricorrente o ripetuto a intervalli costanti;
C. che avviene in modo costante o a intervalli periodici.

L'aggettivo "**sistematico**" ha almeno uno dei seguenti significati a giudizio del Working Party:

A. che avviene per sistema;
B. predeterminato, organizzato o metodico;
C. che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;
D. svolto nell'ambito di una strategia.

MONITORAGGIO REGOLARE E SISTEMATICO DEGLI INTERESSATI

Le linee guida forniscono anche alcune utili esemplificazioni di attività di monitoraggio sistematico e regolare, tra le quali:

A. il curare il funzionamento di una rete di telecomunicazioni; la prestazione di servizi di telecomunicazioni;
B. il tracciamento dell'ubicazione, per esempio da parte di app su dispositivi mobili;
C. i programmi di fidelizzazione;
D. l'utilizzo di telecamere a circuito chiuso;
E. i dispositivi connessi quali contatori intelligenti, automobili intelligenti, dispositivi per la domotica.

Dalle Nuove Faq sul Responsabile della Protezione dei Dati (RPD) in ambito privato Pubblicate dal Garante per la Protezione dei Dati Personali del 26/03/2018

Chi sono i soggetti privati obbligati alla sua designazione?

Ricorrendo i suddetti presupposti, sono tenuti alla nomina, a titolo esemplificativo e non esaustivo:

Dalle Nuove Faq sul Responsabile della Protezione dei Dati (RPD) in ambito privato Pubblicate dal Garante per la Protezione dei Dati Personali del 26/03/2018

- istituti di credito;
- imprese assicurative;
- sistemi di informazione creditizia;
- società finanziarie;
- società di informazioni commerciali;
- società di revisione contabile;
- società di recupero crediti;
- istituti di vigilanza;
- partiti e movimenti politici; sindacati; caf e patronati;
- società operanti nel settore delle "utilities" (telecomunicazioni, distribuzione di energia elettrica o gas);

Dalle Nuove Faq sul Responsabile della Protezione dei Dati (RPD) in ambito privato Pubblicate dal Garante per la Protezione dei Dati Personali del 26/03/2018

- società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione;
- società di call center;
- società che forniscono servizi informatici;
- società che erogano servizi televisivi a pagamento.

Dalle Nuove Faq sul Responsabile della Protezione dei Dati (RPD) in ambito privato Pubblicate dal Garante per la Protezione dei Dati Personali del 26/03/2018

Chi sono i soggetti per i quali non è obbligatoria la designazione del responsabile della protezione dei dati personali: Nei casi diversi da quelli previsti dall'art. 37, par. 1, lett. b) e c), del Regolamento (UE) 2016/679 ad esempio:

- in relazione a trattamenti effettuati da liberi professionisti operanti in forma individuale; agenti, rappresentanti e mediatori operanti non su larga scala; imprese individuali o familiari; piccole e medie imprese, con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti: v. anche considerando 97 del Regolamento, in relazione alla definizione di attività "accessoria"

Il Responsabile della protezione dei dati

(Data Protection Officer)

✓Il DPO va designato in funzione delle **qualità professionali,** della **conoscenza specialistica della normativa** e delle **prassi in materia di protezione dei dati**, e della **capacità di assolvere i propri compiti.**

✓E' **figura apicale**, assolutamente diversa quanto a ruolo e funzioni dal "semplice" responsabile del trattamento.

✓Un **gruppo** imprenditoriale **può nominare un unico** DPO.

✓I **dati di contatto** del DPO vanno **comunicati al Garante per la protezione dei dati personali e resi pubblici**.

✓**Può essere un dipendente** del Titolare o del Responsabile del trattamento *oppure* **un consulente esterno** che assolve i suoi compiti in base a un **contratto di servizi.**

Il Responsabile della protezione dei dati

✓ Il DPO deve essere **autonomo ed indipendente**:

- non deve ricevere dal Titolare o dal Responsabile alcuna istruzione per quanto riguarda l'esecuzione dei compiti affidati **né è soggetto a potere disciplinare o sanzionatorio** per l'adempimento dei propri compiti.
- Il DPO non dovrà avere conflitti di interesse in azienda e dovrà essere coinvolto preventivamente nelle decisioni del management

- Il DPO deve poter accedere ai dati personali e ai trattamenti, dovrà ricevere supporto adeguato in termini di risorse finanziarie, infrastrutturali e, ove opportuno, di personale e risorse.) necessarie per l'espletamento dei propri compiti, (es. (personale, locali, attrezzature, ecc, aggiornamento professionale per mantenere le proprie conoscenze specialistiche.

Il Responsabile della protezione dei dati

(Data Protection Officer)

- Il Regolamento individua il **nucleo minimo** dei compiti assegnati al DPO:

✓ **Informare e fornire** al Titolare, al Responsabile nonché ai dipendenti che eseguono il trattamento, **consulenza** in merito agli obblighi normativi in materia;

Il Responsabile della protezione dei dati

- ✓ **Sorvegliare l'osservanza della normativa** in materia di protezione dei dati personali nonché delle **politiche** in materia del Titolare o del Responsabile del trattamento, compresi l'attribuzione di responsabilità, la sensibilizzazione e formazione del personale che partecipa al trattamento e al controllo in merito;
- ✓ **Fornire,** se richiesto, **pareri** sulla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
- ✓ **Cooperare** con l'Autorità di controllo;
- ✓ **Fungere da punto di contatto con il Garante per la protezione dei dati di personali** per questioni connesse al trattamento.

GENERAL SERVICE lab

Formazione - Sicurezza - Compliance

L’informativa all’interessato rafforzata

L'INFORMATIVA ALL'INTERESSATO RAFFORZATA

✓Rispetto all'art. 13 del Codice Privacy, si prevedono **numerose informazioni aggiuntive** da fornire agli interessati in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro.

✓L'Informativa **va resa per iscritto o con altri mezzi, anche elettronici**. Anche **oralmente**, purché sia richiesto dall'interessato e sia comprovata con altri mezzi l'identità dell'interessato.

✓Le informazioni possono essere fornite anche in combinazione con **icone standardizzate** per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un **quadro d'insieme del trattamento previsto**. Se presentate elettronicamente, le icone devono essere leggibili da qualsiasi dispositivo.

L'INFORMATIVA ALL'INTERESSATO RAFFORZATA

Rispetto agli elementi obbligatori da indicare nell'informativa privacy ai sensi dell'art. 13 del Codice Privacy, i Titolari del trattamento dovranno inserire obbligatoriamente anche le seguenti informazioni aggiuntive sul trattamento:

- ✓ i **dati di contatto** della nuova figura del DPO, ove prevista e del Responsabile del trattamento;
- ✓ la **base giuridica del trattamento** a corredo della illustrazione delle finalità del trattamento;
- ✓ qualora il trattamento si basi sulla necessità di perseguire un **legittimo interesse** del titolare del trattamento o di terzi, **la specificazione di quali siano i legittimi interessi** perseguiti dal titolare del trattamento o da terzi;
- ✓ **l'ambito del trasferimento all'estero** (ovviamente extra UE) o a un'organizzazione internazionale dei dati personali;

L'INFORMATIVA ALL'INTERESSATO RAFFORZATA

Il perseguimento di un legittimo interesse si pone come base giuridica alternativa alle altre previste nell'art. 6 del GDPR. **Il titolare che abbia un legittimo interesse può procedere al trattamento anche in assenza del consenso da parte dell'interessato**, di un rapporto contrattuale (o di misure precontrattuali), di obblighi legali, di esigenze di salvaguardia di interessi vitali dell'interessato o di altra persona fisica, di esercizio di poteri pubblici.

il considerando n. 47 del GDPR chiarisce che per la valutazione della sussistenza di un legittimo interesse del titolare deve innanzitutto tenere conto delle "*ragionevoli aspettative dell'interessato in base alla sua relazione con il titolare del trattamento*"

L'INFORMATIVA ALL'INTERESSATO RAFFORZATA

Il perseguimento di un legittimo interesse si pone come base giuridica alternativa alle altre previste nell'art. 6 del GDPR. **Il titolare che abbia un legittimo interesse può procedere al trattamento anche in assenza del consenso da parte dell'interessato**, di un rapporto contrattuale (o di misure precontrattuali), di obblighi legali, di esigenze di salvaguardia di interessi vitali dell'interessato o di altra persona fisica, di esercizio di poteri pubblici.

il considerando n. 47 del GDPR chiarisce che per la valutazione della sussistenza di un legittimo interesse del titolare deve innanzitutto tenere conto delle "*ragionevoli aspettative dell'interessato in base alla sua relazione con il titolare del trattamento*"

L'INFORMATIVA ALL'INTERESSATO RAFFORZATA

- ✓ il **periodo di conservazione** dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- ✓ la **specifica esistenza del diritto alla portabilità dei dati**;
- ✓ l'esistenza del **diritto di revocare il consenso in qualsiasi momento** senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- ✓ il diritto di **proporre reclamo** al Garante per la protezione dei dati personali;

L'INFORMATIVA ALL'INTERESSATO RAFFORZATA

- ✓ la **eventuale esistenza di un processo decisionale automatizzato**, compresa la **profilazione** e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato;

- ✓ la **fonte da cui hanno origine i dati personali** e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico (solo ove i dati non siano raccolti presso l'interessato);

- ✓ le **categorie di dati personali oggetto del trattamento** (solo ove i dati non siano raccolti presso l'interessato).

L'INFORMATIVA ALL'INTERESSATO RAFFORZATA

Nel caso in cui i dati personali oggetto del trattamento non siano raccolti presso l'interessato, l'informativa dovrà essere fornita al più tardi **entro un mese dall'ottenimento** dei dati o, nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato o con un terzo, al più tardi **al momento di tale comunicazione**.

GENERAL SERVICE lab

Formazione - Sicurezza - Compliance

Il consenso al trattamento dei dati personali

IL CONSENSO DELL'INTERESSATO

✓Il consenso dell'interessato rappresenta la **principale precondizione di liceità** del trattamento.

✓Il Titolare deve **poter dimostrare** che l'interessato ha prestato il consenso al trattamento. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso deve **essere presentata in modo chiaramente distinguibile dalle altre materie**, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro, **pena l'invalidità del consenso prestato.**

✓L'interessato ha il **diritto di revocare il proprio consenso in qualsiasi momento** con modalità di esecuzione della revoca del consenso facili come la sua prestazione originaria.

IL CONSENSO DELL'INTERESSATO

✓È **specificatamente vietato** che l'esecuzione di un contratto o la prestazione di un servizio siano condizionati alla prestazione del consenso al trattamento di dati personali **non necessario** all'esecuzione del contratto o servizio.

Alla **specifica manifestazione del consenso** è in particolare subordinata:

(i) la liceità del trattamento (altrimenti vietato, salvo eccezioni) dei dati personali "particolari";

(ii) la possibilità – **altrimenti vietata** – di procedere alla **profilazione dell'interessato**;

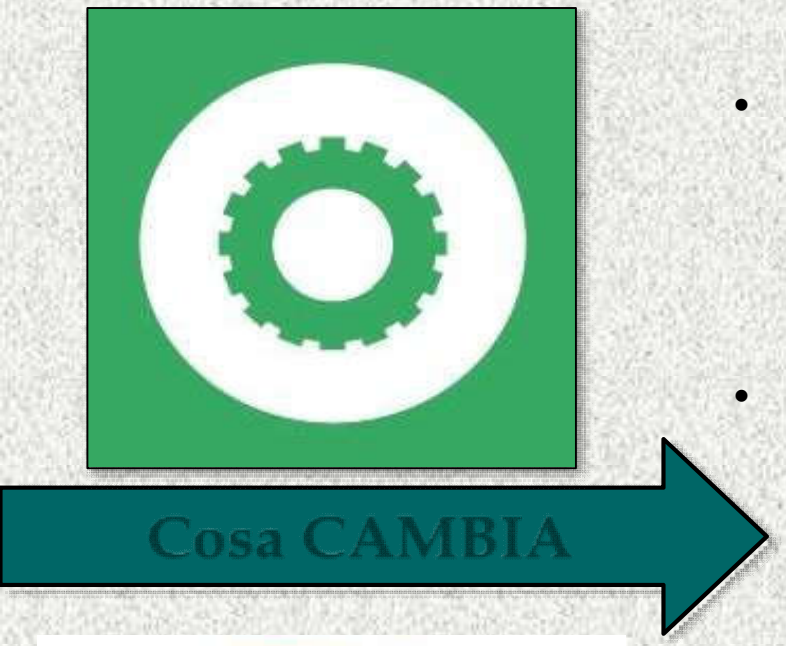
(iii) la possibilità di **trasferire i dati personali dell'interessato verso un Paese terzo extra UE** o verso un'organizzazione internazionale.

IL CONSENSO E I MINORI D'ETÀ

✓Se un trattamento di dati nell'ambito **della fornitura ad un minore di un servizio della società dell'informazione** (es. l'accesso a Internet, l'iscrizione a un social network, etc.) prevede l'acquisizione del consenso preventivo, la **raccolta del consenso e il trattamento dei dati del minore sono leciti se egli abbia compiuto almeno 16 anni** (salvo il diritto degli Stati membri di stabilire anche un'età inferiore a tali fini, purché non inferiore ai 13 anni)

✓Il Titolare deve adottare **misure ragionevoli per verificare che il consenso sia prestato** o autorizzato dal titolare della potestà genitoriale sul minore.

Il Consenso
Cosa Cambia



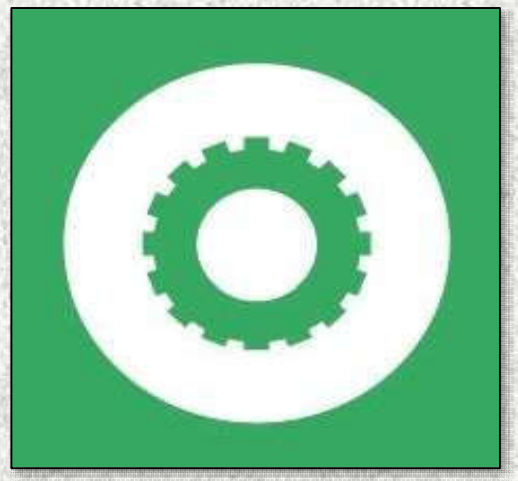
- **DEVE essere ESPLICITO** per i **DATI SENSIBILI** (si veda art. 9 Regolamento), anche per le **DECISIONI** basate su **TRATTAMENTI AUTOMATIZZATI (compresa la profilazione – art. 22).**

- NON deve essere necessariamente DOCUMENTATO PER ISCRITTO, né è richiesta la "forma scritta", anche se questa è modalità idonea a configurare l'inequivocabilità del consenso e il suo essere esplicito (per i dati sensibili).

- **Il Titolare (art. 7.1) DEVE essere in grado di DIMOSTRARE** che l'Interessato ha prestato il consenso a uno specifico Trattamento..

- **Il consenso dei MINORI è valido a partire dai SEDICI ANNI:** prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci.

Il Consenso
Cosa è Invariato



Cosa è INVARIATO

- **DEVE ESSERE**, in tutti i casi, **LIBERO, SPECIFICO, INFORMATO E INEQUIVOCABILE**
- **NON È AMMESSO IL CONSENSO TACITO O PRESUNTO** (no a caselle pre-spuntate su un modulo).
- **DEVE ESSERE MANIFESTATO attraverso una apposita dichiarazione o azione positiva inequivocabile** (gli approfondimenti sono riportati nei considerando 39 e 42 del regolamento)

GENERAL SERVICE lab

Formazione - Sicurezza - Compliance

Il Registro generale delle attività di trattamento svolte

IL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

✓**Imprese o organizzazioni con numero di dipendenti pari o superiore a 250:** deve essere redatto (anche in formato elettronico) sia dal Titolare che dal Responsabile del trattamento e **va esibito** su richiesta al Garante per la protezione dei dati personali;

✓Imprese **con meno di 250 dipendenti:** obbligo di redazione se il trattamento da esse svolto (i) presenta un rischio per i diritti e le libertà dell'interessato; (ii) non è occasionale o include dati personali "particolari" o relativi a condanne penali e reati.

✓Rappresenta l'elemento fondamentale in relazione all'obbligo di elaborare un **sistema documentale di gestione della privacy** contenente tutti gli atti, regolarmente aggiornati, redatti per soddisfare i requisiti di conformità al Regolamento (**"*accountability*")**

IL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Ove redatto dal **Titolare del trattamento**, il Registro generale contiene:

a) Nome e dati di contatto del Titolare, contitolare, rappresentante del Titolare e DPO;

b) Finalità del trattamento;

c) Categorie di interessati e di dati personali;

d) Ambito di comunicazione, anche verso Paesi terzi;

e) Ove possibile, i termini ultimi per la cancellazione delle diverse categorie dei dati;

f) Ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.

IL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Ove redatto dal **Responsabile del trattamento**, il Registro generale contiene:

a) Nome e dati di contatto del/i Responsabile/i, del Titolare per cui egli agisce, del rappresentante del Titolare o del Responsabile e del DOP;

b) Categorie dei trattamenti effettuati per conto di ogni Titolare;

c) ove applicabile, i trasferimenti di dati personali verso un Paese terzo o un'organizzazione internazionale identificati e eventuali garanzie;

d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.

GENERAL SERVICE lab

Formazione - Sicurezza - Compliance

VALUTAZIONE DI IMPATTO PRIVACY

La DPIA
(Data Protection Impact Assesment)

La **valutazione d'impatto sulla protezione dei dati** altro non è che un processo volto a descrivere un trattamento di dati personali, valutarne la necessità e la proporzionalità, nonché gestirne gli eventuali rischi per i diritti e le libertà delle persone fisiche da esso derivanti, effettuando una valutazione del livello del rischio e determinando le misure idonee a mitigarlo.

La DPIA
(Data Protection Impact Assesment)

Il DPIA va inquadrato come uno strumento essenziale e fondamentale per tutti i titolari e responsabili del trattamento al fine di dar corso al nuovo approccio alla protezione dei dati personali voluto dal legislatore comunitario e fortemente basato sul principio della responsabilizzazione (cd. accountability principle).

L'articolo 35, comma 1, del GDPR prevede che il processo di DPIA sia obbligatorio quando un trattamento di dati personali "presenti un rischio elevato per i diritti e le libertà delle persone fisiche"

La DPIA
(Data Protection Impact Assesment)

Il DPIA va inquadrato come uno strumento essenziale e fondamentale per tutti i titolari e responsabili del trattamento al fine di dar corso al nuovo approccio alla protezione dei dati personali voluto dal legislatore comunitario e fortemente basato sul principio della responsabilizzazione (cd. accountability principle).

L'articolo 35, comma 1, del GDPR prevede che il processo di DPIA sia obbligatorio quando un trattamento di dati personali "presenti un rischio elevato per i diritti e le libertà delle persone fisiche"

La DPIA
(Data Protection Impact Assesment)

l'articolo 35, comma 3, del GDPR fornisce alcuni esempi di casi nei quali un trattamento di dati personali "possa presentare rischi elevati": (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 (articolo 9 del GDPR) o di dati relativi a condanne penali e a reati (cfr. articolo 10 del GDPR); (c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico

La DPIA
(Data Protection Impact Assesment)

l'articolo 35, comma 3, del GDPR fornisce alcuni esempi di casi nei quali un trattamento di dati personali "possa presentare rischi elevati": (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 (articolo 9 del GDPR) o di dati relativi a condanne penali e a reati (cfr. articolo 10 del GDPR); (c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico

La DPIA
(Data Protection Impact Assesment)

Ad ogni modo si precisa che, qualora dovesse risultare poco chiaro se una situazione richieda o meno lo svolgimento del DPIA, la raccomandazione del WP-29 è quella di effettuarlo comunque, in quanto risulta essere, in ogni caso, uno strumento utile per i titolari del trattamento al fine di rispettare la legge in materia di protezione dei dati.

GENERAL SERVICE lab

Formazione - Sicurezza - Compliance

Trasferimento dei dati fuori dell'Unione Europea.

TRASFERIMENTO DEI DATI PERSONALI EXTRA UE

Il Regolamento non introduce particolari novità rispetto all'attuale quadro

Condizioni di liceità:

✓**trasferimento sulla base di una decisione di adeguatezza** (ove la Commissione UE abbia deciso che il Paese terzo, un territorio o uno o più settori specifici all'interno del Paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato; in tal caso il trasferimento non necessita di autorizzazioni specifiche);

✓**trasferimento soggetto a garanzie adeguate** (il Titolare o il Responsabile del trattamento può trasferire dati personali verso un Paese terzo o un'organizzazione internazionale solo se ha fornito garanzie adeguate, come ad esempio le norme vincolanti d'impresa, le clausole contrattuali standard, l'esistenza di un codice di condotta, l'esistenza di un meccanismo di certificazione, specifiche clausole contrattuali).

TRASFERIMENTO DEI DATI PERSONALI EXTRA UE

In assenza delle suddette condizioni, il trasferimento è ammesso **soltanto** se si verifica **una** delle seguenti condizioni:

a) l'interessato, debitamente informato, abbia **acconsentito** esplicitamente al trasferimento;

b) il trasferimento sia necessario all'esecuzione di un **contratto** o all'esecuzione di **misure precontrattuali adottate su istanza dell'interessato**;

c) il trasferimento sia necessario alla conclusione o esecuzione di un **contratto** stipulato tra il Titolare e un terzo **a favore dell'interessato**;

d) il trasferimento sia necessario per importanti **motivi di pubblico interesse**;

e) il trasferimento sia necessario per accertare, esercitare o difendere un **diritto in sede giudiziaria**;

f) il trasferimento sia necessario per **tutelare gli interessi vitali dell'interessato o di terzi**, qualora l'interessato si trovi nell'impossibilità fisica o giuridica di prestare consenso;

g) il trasferimento sia effettuato a partire da un **registro pubblico.**

GENERAL SERVICE lab

Formazione - Sicurezza - Compliance

I diritti dell'interessato: il diritto all'oblio

DIRITTO ALL'OBLIO

✓**Oggetto**: Diritto dell'interessato ad ottenere, senza giustificato ritardo, la **cancellazione** dei propri dati personali che (i) **non siano più necessari** per le finalità per le quali sono stati raccolti o altrimenti trattati, o (ii) quando l'interessato abbia **revocato il proprio consenso**, o (iii) si sia **opposto al trattamento** dei dati personali che lo riguardano, o (iv) quando il trattamento dei suoi dati personali **non sia altrimenti conforme al Regolamento**.

✓Il Titolare del trattamento che **ha pubblicato on line dati personali deve informare gli altri Titolari del trattamento che trattano tali dati personali di cancellare qualsiasi link** verso tali dati personali o copia o riproduzione di detti dati.

✓Il Titolare può opporsi solo in caso di: esercizio del diritto alla libertà di espressione e di informazione; per adempiere un obbligo legale o un compito di interesse pubblico; per motivi di interesse pubblico nel settore della sanità pubblica; a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici; per accertare, esercitare o difendere un diritto in sede giudiziaria.

GENERAL SERVICE lab

Formazione - Sicurezza - Compliance

I diritti dell'interessato: il diritto alla portabilità dei dati

IL DIRITTO ALLA PORTABILITÀ DEI DATI

✓**Oggetto:** diritto dell'interessato di **trasmettere o ottenere la trasmissione di propri dati personali da un Titolare del trattamento a cui li aveva forniti in precedenza ad un altro Titolare**, senza impedimenti;

✓Tale diritto è esercitabile quando: (i) il trattamento è effettuato con mezzi automatizzati; e (ii) il trattamento si basa sul consenso precedentemente rilasciato dall'interessato; o (iii) il trattamento si basa su un contratto o su trattative precontrattuali in corso con l'interessato.

✓L'interessato ha il diritto di **ottenere in formato strutturato**, di uso comune e leggibile da dispositivo automatico, i propri dati personali al fine di trasmetterli a un altro Titolare, ma anche il diritto di ottenere che il primo Titolare a cui ha fornito i dati, li **trasmetta direttamente** a un diverso Titolare, se tecnicamente fattibile.

GENERAL SERVICE lab

Formazione - Sicurezza - Compliance

DATA BREACH

Violazione di Dati Personali (Data Breach)

✓L'art. 33 del **Regolamento Europeo 679/2016** (**GDPR**) impone al titolare del trattamento di notificare all'autorità di controllo la violazione di dati personali (**data breach**) entro settantadue ore dal momento in cui ne viene a conoscenza.

✓L'obbligo di notifica scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche, qualora, poi, il rischio fosse elevato, allora, oltre alla notifica, il titolare è tenuto a darne comunicazione all'interessato.

Violazione di Dati Personali (Data Breach)

✓L'eventuale ritardo nella notificazione deve essere giustificato, il mancato rispetto dell'obbligo di notifica, invece, pone l'autorità di controllo nella condizione di applicare le misure correttive a sua disposizione ovvero: l'esercizio dei poteri previsti dall'art.58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati), la imposizione di sanzioni amministrative secondo l'art. 83 GDPR, il cui importo può arrivare a 10.000.000 di euro o al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

GENERAL SERVICE lab

Formazione - Sicurezza - Compliance

Autorità di controllo e Strumenti di tutela

L'AUTORITÀ DI CONTROLLO

✓**L'Autorità di Controllo sorveglia l'applicazione del Regolamento** al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno della UE;

✓Ogni Stato membro **nomina** tra le proprie autorità pubbliche indipendenti la propria Autorità di Controllo attraverso una procedura **trasparente**: in Italia, il **Garante per la protezione dei dati personali;**

✓Le Autorità di Controllo dei vari Stati membri **cooperano** e si scambiano informazioni e **assistenza reciproca** per attuare e applicare il Regolamento in modo coerente;

✓L'Autorità di Controllo ha **poteri di indagine, correttivi, autorizzativi, consultivi**, il cui esercizio è soggetto a garanzie adeguate. **Annualmente** deve redigere una **relazione** di attività che trasmette al Parlamento, Governo e altre autorità designate dal diritto nazionale.

STRUMENTI DI TUTELA

- ✓ **Reclamo all'Autorità di controllo** dello Stato di residenza abituale dell'interessato-reclamante o del luogo ove si è verificata la presunta violazione.
- ✓ **Ricorso giurisdizionale effettivo** avverso decisione dell'Autorità di Controllo.
- ✓ **Ricorso giurisdizionale effettivo** nei confronti del Titolare o del Responsabile del trattamento in caso di violazione di diritti tutelati dal Regolamento.

GENERAL SERVICE lab

Formazione - Sicurezza - Compliance

Il nuovo apparato sanzionatorio

RESPONSABILITÀ CIVILE

✓Dal punto di vista **civilistico**, confermata la <u>responsabilità risarcitoria</u> per il c.d. "*danno da trattamento*": l'art. 82 prescrive difatti che "*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*".

✓Chiariti i meccanismi di ripartizione della responsabilità risarcitoria tra Titolare e Responsabile del trattamento, e tra contitolari del trattamento (con la previsione specifica di azioni di regresso reciproche), così come i meccanismi di esonero.

:

SANZIONI AMMINISTRATIVE

1. fino a **10.000.000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente**, se superiore, nel caso di violazione di determinati obblighi posti dal Regolamento;

2. fino a **20.000.000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente**, se superiore, nel caso di violazione degli obblighi più stringenti posti dal Regolamento (anche nel semplice caso di inosservanza degli ordini del Garante);

✓ Le sanzioni amministrative pecuniarie sono inflitte **in aggiunta o in luogo alle sanzioni di cui all'art. 58, par. 2, lett. da a) a h) e j) del Regolamento** (avvertimenti, ammonimenti, ingiunzioni,limitazioni ai trattamenti, ordine di cancellazione, rettifica o limitazioni del trattamento, revoca della certificazione o ingiunzione all'Organismo certificatore di ritirare o non emettere la certificazione, ordine di sospensione dei flussi di dati verso un destinatario)

SANZIONE AMMINISTRATIVA PECUNIARIA	DISPOSIZIONE VIOLATA	OBBLIGO VIOLATO (in sintesi)
Fino a **20.000.000 EUR** o, per le imprese, fino al **4%** del fatturato mondiale totale annuo dell'esercizio precedente, se superiore	**Art. 5**	Rispetto dei principi applicabili al trattamento liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.
	Art. 6	Rispetto delle condizioni di liceità del trattamento
	Art. 7	-Dimostrazione della prestazione del consenso e del rispetto delle condizioni per il consenso. - Tutela del dritto dell'interessato di revoca del consenso
	Art. 9	Rispetto delle condizioni di liceità del trattamento di categorie particolari di dati personali
	22	-Obblighi informativi nei confronti dell'interessato - Tutela dei diritti dell'interessato (diritto d'accesso; di rettifica; all'oblio; di **Artt. da 12 a** limitazione del trattamento; di notifica in caso di rettifica o cancellazione dei dati o limitazione del trattamento; alla portabilità dei dati; di opposizione ; alla profilazione consenziente)
	Artt. da 44 a 49	Obblighi connessi al trasferimento di dati personali verso Paesi terzi o organizzazioni internazionali
	Capo IX	Qualsiasi obbligo previsto dalle legislazioni degli Stati membri per specifiche situazioni di trattamento a norma del Capo IX del Regolamento
	Art. 58	Rispetto di un ordine, di una limitazione di trattamento o di un ordine di sospensione di flussi di dati dell'Autorità di controllo o di un negato accesso ai sensi dell'art. 58, par. l

GENERAL SERVICE lab
Formazione - Sicurezza - Compliance

Assioma Group S.r.l.

STUDIO LEGALE PALMA
lawers & consultans
avv. Francesco Palma

GENERAL SERVICE soc. coop.
SICUREZZA - SALUTE - QUALITA' - AMBIENTE - FORMAZIONE

GRAZIE DELL'ATTENZIONE