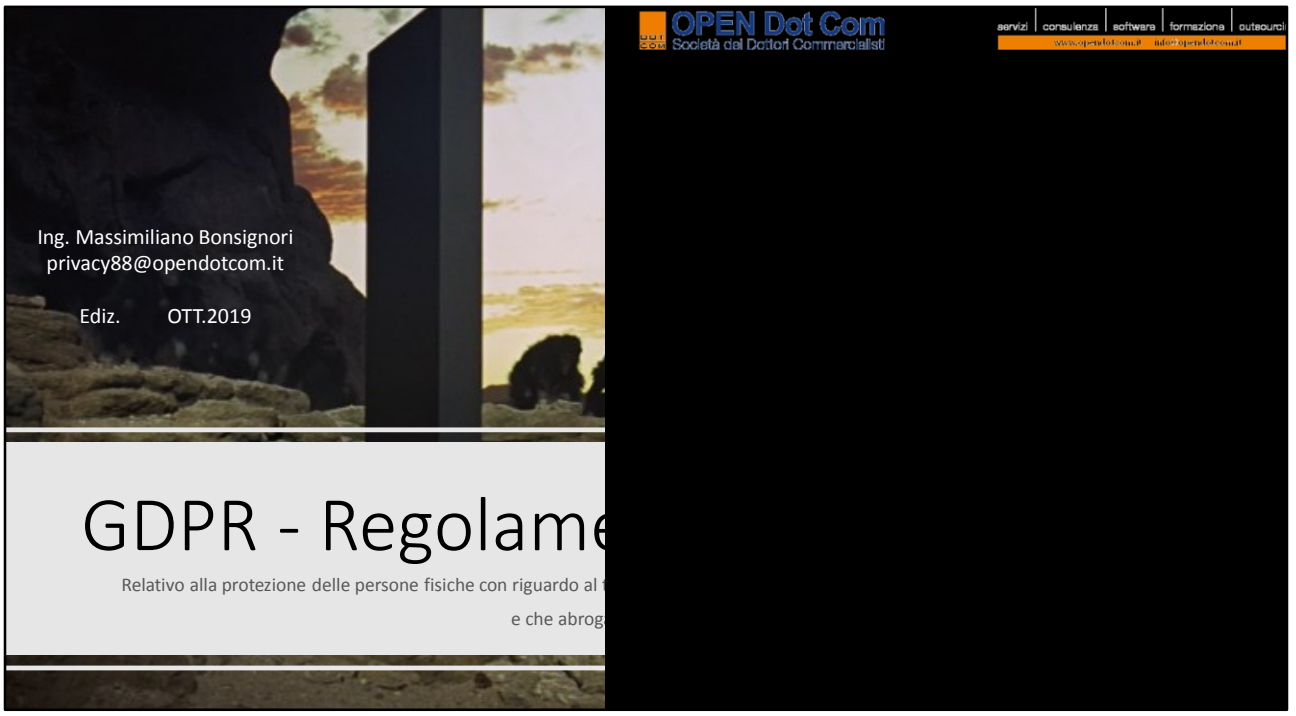
Prima di cominciare, un breve sondaggio…

grazie per la collaborazione



Il presente corso riguarda il Regolamento Europeo n. 679 del 27/04/2016 pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 04/05/2016, 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, entrato in vigore il 25/05/2018.

Tale regolamento è noto sotto l'acronimo GDPR che sta per General Data Protection Regulation ovvero Regolamento generale per la protezione dei dati. E' bene però subito sgombrare il campo dagli equivoci: in inglese si parla di "privacy", ma è fuorviante. Il regolamento fa riferimento a dati riferibili a persone identificate o identificabili

Era da anni, sin dal 2010, che in sede europea si parlava di una riforma nella normativa privacy per aggiornare i principi enunciati nella direttiva del 1995, in modo da tenere il passo con i grandi cambiamenti nel trattamento dei dati apportati da Internet e globalizzazione (es. social networks, shopping on-line e servizi di e-banking), dalle sfide per la

sicurezza e il controllo antiterrorismo, dalla maggiore coesione territoriale e traffico transfrontaliero e dallo sviluppo del mercato unico.

Le finalità dichiarate che accompagnano questo nuovo regolamento sono:
-porre rimedio al disomogeneo recepimento da parte degli Stati membri della direttiva 95/46/CE
-sostituire gli obblighi di tipo formale e burocratico con attività finalizzate ad una maggiore responsabilizzazione e consapevolezza dei rischi;
-introdurre nuovi diritti a tutela delle persone;
-rispondere alle sfide poste dagli sviluppi tecnologici e dai nuovi modelli di crescita economica, tenendo conto delle esigenze di tutela dei dati personali sempre più avvertite dai cittadini dei Paesi dell'Unione europea

Dal 25/05/2018 le nuove norme, sancite nel GDPR, sono applicabili in tutta l'Unione Europea prevalgono sulle normative nazionali previgenti, adottate ai sensi della direttiva abrogata.

Infatti, anche se il Regolamento è direttamente applicabile e vincolante in tutti gli Stati membri dell'Unione europea, in quanto non richiede una legge di recepimento nazionale, diverse sue disposizioni lasciano liberi gli Stati Membri - o richiedono agli stessi - di introdurre ulteriori regole e condizioni

Gli Stati hanno avuto due anni per porre in essere gli adeguamenti richiesti dalla normativa in questione alle proprie politiche per la protezione ed il trattamento dei dati personali. Infatti, oltre al Regolamento, del pacchetto di riforma, fa parte una Direttiva indirizzata alla regolamentazione dei settori di prevenzione, contrasto e repressione dei crimini, nonché all'esecuzione delle sanzioni penali.

Esistono dei campi d'azione in cui il regolamento cede il passo alla normativa nazionale, laddove manca un'armonia a livello sovranazionale.
Ad esempio i concetti di "giornalismo" e "libertà di espressione"

continueranno a variare da uno Stato membro all'altro, così come la gestione dei dati elaborati ai fini della sicurezza nazionale di uno Stato. Guardando nello specifico all'Italia, in ambito trasparenza, la nuova disciplina del cosiddetto Freedom of Information Act (FOIA) nella pubblica amministrazione sembrerebbe doversi conciliare con il Regolamento, ma non si dice come.

In Italia, dal 19/09/2018, è in vigore la versione aggiornata Decreto legislativo del 30 giugno 2003 n. 196, noto come Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al 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, come integrazioni e modifiche introdotte dal
Decreto legislativo del 10 agosto 2018, n. 101.
Termina così il periodo di *vacatio legis* intercorso dal 25/05/2018 al 18/09/2018 venutosi a creare con il ritardo con cui il legislatore ha dato seguito all'obbligo di armonizzazione della legislazione nazionale a quella europea.
Non è stabilito alcun periodo di cosiddetta applicazione "soft" delle disposizioni in essa contenute, né da parte della Autorità Garante né da parte di chiunque altro sia tenuto ad applicare e far applicare questo decreto legislativo. Ci si limita invece a raccomandare al Garante, solo ai fini della applicazione di eventuali sanzioni, di tenere conto per otto mesi dalla entrata in vigore del decreto, fino al 19/05/2015, «della fase di prima applicazione delle norme sanzionatorie»

Dunque, è l'intera normativa italiana in materia di tutela dei dati personali che va letta, interpretata e applicata in un quadro estremamente complesso che comprende il GDPR e il Codice oggetto del d.lvo 196 del 2003 come novellato dal d.lvo 101 del 2018.
Da tenere sempre presente è che tutta la normativa italiana in materia, sia quella contenuta nel d.lvo n. 196 del 2003 e non abrogata o modificata dal d.lvo n. 101 del 2018, sia quella contenuta in questo ultimo, nuovo, decreto, deve essere interpretata e applicata alla luce del GDPR e in conformità alle sue norme

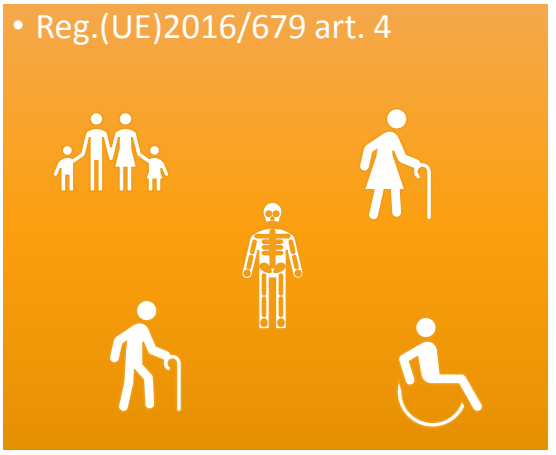

GDPR
General Data Protection Regulation


INTERESSATI
ORGANIZ-
ZAZIONE
GARANTE

Dato personale

- qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»);

- Reg.(UE)2016/679 art. 4

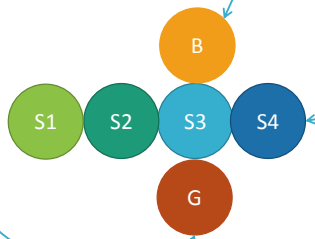


Dato personale

Si intende per Dato personale qualsiasi informazione riguardante una persona fisica identificata o identificabile
Tale persona è detta «interessato» in italiano, «data subject» in inglese

Categorie particolari di dati personali

- (G) Dati genetici
- (B) Dati biometrici (identificativi)



- Dati Sensibili (ex D.Lgs 196/03)
- Si tratta di dati personali "umani" idonei a rivelare:
  - (S1) l'origine razziale ed etnica
  - (S2) le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale
  - (S3) lo stato di salute
  - (S4) la vita sessuale

Gruppo di studio sicurezza e privacy 8

In sintesi si tratta dei «vecchi» dati sensibili, del previgente codice privacy, a cui si aggiungono quelli genetici e biometrici
Come si può osservare nel diagramma a palle
(S1) l'origine razziale ed etnica
(S2) le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale
(S3) lo stato di salute
(S4) la vita sessuale
(G) Dati genetici
(B) Dati biometrici (identificativi)

Dati relativi a condanne penali e reati o a connesse misure di sicurezza

d.lgs.196/2003 art. 4 dati personali giudiziari	Reg.(UE)2016/679 art. 10
• i dati personali idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi del codice di procedura penale	• Dati relativi a condanne penali e reati o a connesse misure di sicurezza

Dati relativi a condanne penali e reati o a connesse misure di sicurezza

I dati personali di cui all'art.10 del GDPR sono quei Dati relativi a condanne penali e reati o a connesse misure di sicurezza
Che subentrano ai «vecchi» dati giudiziari, che nel previgente codice privacy erano definiti come quei dati personali idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi del codice di procedura penale

Dati anonimi

- Quei dati che in origine, o a seguito di trattamento, non possono essere in nessun modo associati ad un interessato identificato o identificabile.
- **Quindi non sono dati personali**

Dati pseudonimi

- Quei dati personali che non possono più essere attribuiti a un interessato specifico **senza l'utilizzo di informazioni aggiuntive**, conservate separatamente e soggette a misure tecniche e organizzative adeguate a garantire tale separazione

Dati anonimi e Dati pseudonimi

Sono anonimi Quei dati che in origine, o a seguito di trattamento, non possono essere in nessun modo associati ad un interessato identificato o identificabile.
Quindi non devono considerarsi dati personali

Sono pseudonimi Quei dati personali che non possono più essere attribuiti a un interessato specifico **senza l'utilizzo di informazioni aggiuntive**; queste informazioni sono conservate separatamente dai dati pseudonimi e soggette a misure tecniche e organizzative adeguate a garantire tale separazione

Tipi di trattamento

Che tipi di trattamento sono definiti?

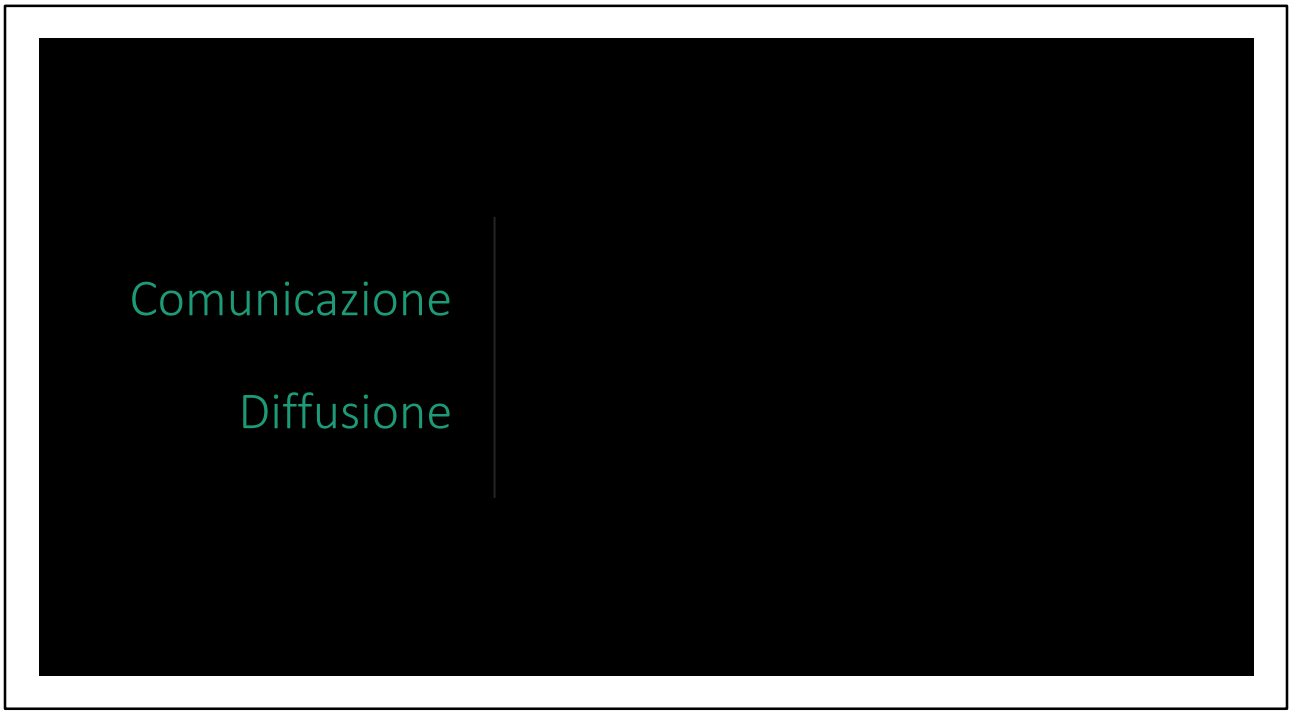
Trattamento

- 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

- Reg.(UE)2016/679 art. 4

Innanzitutto Per Trattamento si intende
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.

Sostanzialmente ogni volta che si «tocca», accede, manipola qualche dato personale si sta eseguendo un trattamento di dati



Comunicazione e Diffusione

Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dai titolari, dai responsabili e dagli autorizzati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione va inteso come **comunicazione**

Sulle figure di titolare, responsabili e autorizzati torneremo a breve; possiamo anticipare che sono quelli che si occupano di trattare i dati entro un perimetro univoco e facente capo ad una struttura definita e coordinata.

Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione, va inteso come **Diffusione**

Profilazione

GPDP, Provvedimento n. 161 del 19 marzo 2015 [doc. web n. 3881513]

- analisi e elaborazione di informazioni relative a utenti o clienti, al fine di suddividere gli interessati in "profili", ovvero in gruppi omogenei per comportamenti o caratteristiche sempre più specifici, con l'obiettivo di pervenire all'identificazione inequivoca del singolo utente (cd. single out) ovvero del terminale e, per il suo tramite, anche del profilo, appunto, di uno o più utilizzatori di quel dispositivo

Reg.(UE)2016/679 art. 4

- 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

Profilazione

La profilazione è una particolare 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.

Nelle provvedimenti del Garante antecedenti si intendevano analisi ed elaborazione di informazioni relative a utenti o clienti, al fine di suddividere gli interessati in "profili", ovvero in gruppi omogenei per comportamenti o caratteristiche sempre più specifici, con l'obiettivo di pervenire all'identificazione inequivoca del singolo utente (cd. single out) ovvero del terminale e, per il suo tramite, anche del profilo, appunto, di uno o più utilizzatori di quel dispositivo

Es. Pubblicità comportamentale

Your Online Choices
a guide to online behavioural advertising

- http://www.youronlinechoices.com/it/le-tue-scelte
- http://www.youronlinechoices.com/it/

Pseudonimizzazione

- il trattamento dei 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;

- Reg.(UE)2016/679 art. 4

Pseudonimizzazione

Si tratta di un trattamento dei dati personali tale per cui 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; Quindi si ottengono dati pseudonimi a partire da dati personali, di solito separando quelli identificativi.

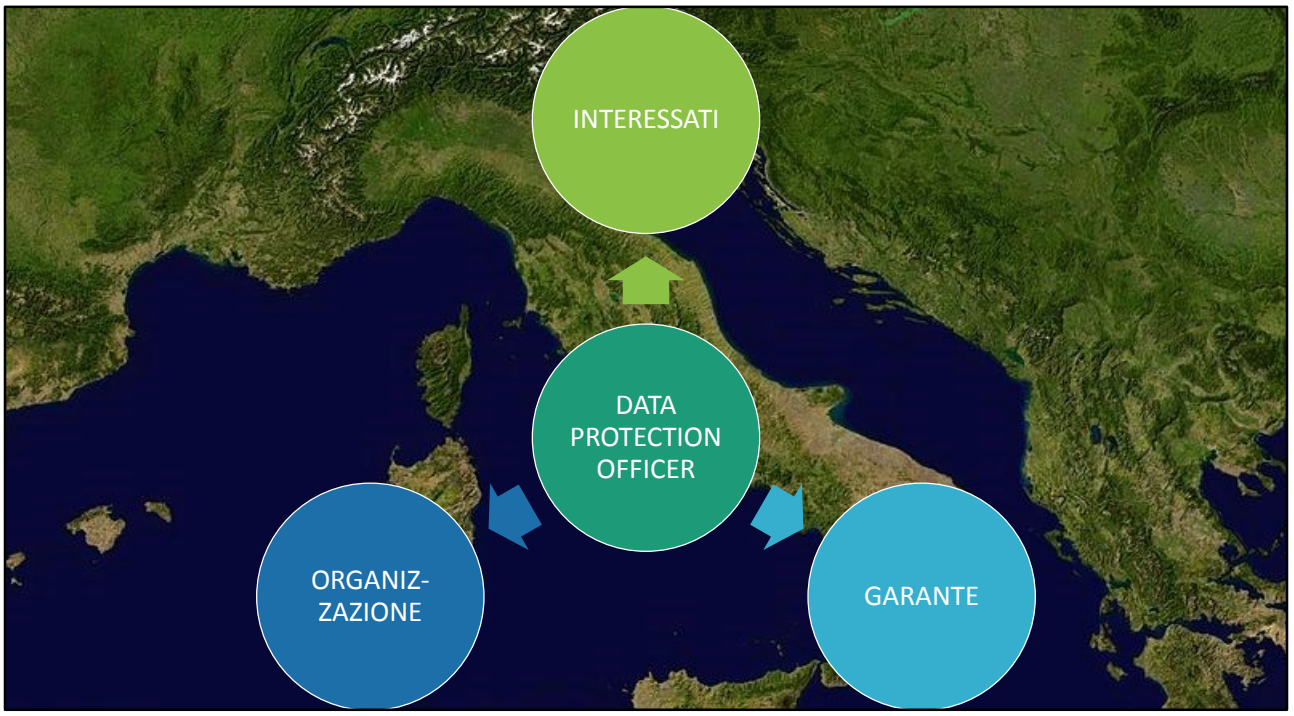
Può essere anche considerata una misura di sicurezza per garantire la riservatezza.

Ruoli

Passiamo ora ai ruoli coinvolti nel trattamento dei dati personali

Ci sono Soggetti (attivi) che effettuano il trattamento
E Soggetti (passivi) che subiscono il trattamento
Questi ultimi, come già visto sono gli interessati o data subjects

Quindi è «interessato» la persona fisica identificata o identificabile


INTERESSATI
DATA PROTECTION OFFICER
ORGANIZ-ZAZIONE
GARANTE

Responsabile della protezione dei dati (RPD ovvero DPO=Data Protection Officer)

- la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo designato dal titolare o dal responsabile affinché sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali

- Reg.(UE)2016/679 artt. 37-39

Responsabile della protezione dei dati - Data Protection Officer

Il Responsabile della protezione dei dati o RPD in italiano
Il Data Protection Officer ovvero DPO in inglese
È una nuova figura Che Affianca sia il titolare, sia il responsabile del trattamento
in alcuni casi è Obbligatoria

Si tratta della persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo designato dal titolare (anche da più contitolari congiuntamente) o dal responsabile affinché sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali

L'unico riferimento nel previgente Codice ad una figura solo in parte sovrapponibile al Responsabile della protezione dei dati è quello al responsabile per il riscontro all´interessato in caso di esercizio dei diritti dell'interessato.

Nell’esecuzione dei suoi compiti, che vedremo a breve, il DPO non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti
Inoltre, riferisce direttamente al vertice gerarchico e non può essere rimosso o penalizzato per l'adempimento dei propri compiti

Va anche detto che il DPO può svolgere altri compiti e funzioni a meno che non diano adito a un conflitto di interessi

> Se si volesse azzardare un parallelo è Simile alla figura del RSPP nella sicurezza sul lavoro

Sono Compiti del DPO

1. informare e fornire consulenza al titolare o al responsabile nonché agli incaricati responsabile del trattamento in merito agli obblighi derivanti dal regolamento nonché da altre disposizioni di legge relative alla protezione dei dati;
2. sorvegliare l'osservanza dei predetti obblighi nonché delle politiche adottate in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo
3. fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento
4. cooperare con l'autorità di controllo
5. fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui
6. effettuare, se del caso, consultazioni relativamente a qualunque altra questione

Tutto ciò considerando debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo

Titolare del trattamento (data controller)

- 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

- Reg.(UE)2016/679 art. 4

Titolare del trattamento (data controller)

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 è il titolare del trattamento

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

Contitolari del trattamento

- due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento

- Reg.(UE)2016/679 art. 26

Quando due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento si dicono Contitolari del trattamento e devono seguire le disposizioni dell'art. 26 del GDPR

i contitolari determinano in modo trasparente, mediante un **accordo** interno (a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti),

1. le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e
2. le rispettive funzioni di comunicazione delle informative

L'accordo può designare un punto di contatto per gli interessati
L'accordo riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati.
Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

Responsabile del trattamento (data processor)

- la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali **per conto** del titolare del trattamento
- se un responsabile del trattamento viola il regolamento, determinando le finalità e i mezzi del trattamento, va considerato titolare del trattamento in questione

- Reg.(UE)2016/679 art. 4, art. 28 co.10

Responsabile del trattamento (data processor)

la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali **per conto** del titolare del trattamento è definita Responsabile del trattamento;
Diversamente a prima i responsabili non vanno più considerati come soggetti interni al titolare e da questi **preposti** al trattamento di dati personali, bensì come outsourcer, fornitori, appaltatori o partner.

se un responsabile del trattamento viola il regolamento, determinando le finalità e i mezzi del trattamento, va considerato titolare del trattamento in questione

Autorizzati trattamento (persons authorized)

- le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile

- Reg.(UE)2016/679 art. 4

Autorizzati trattamento (persons authorized)

Si tratta delle persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile

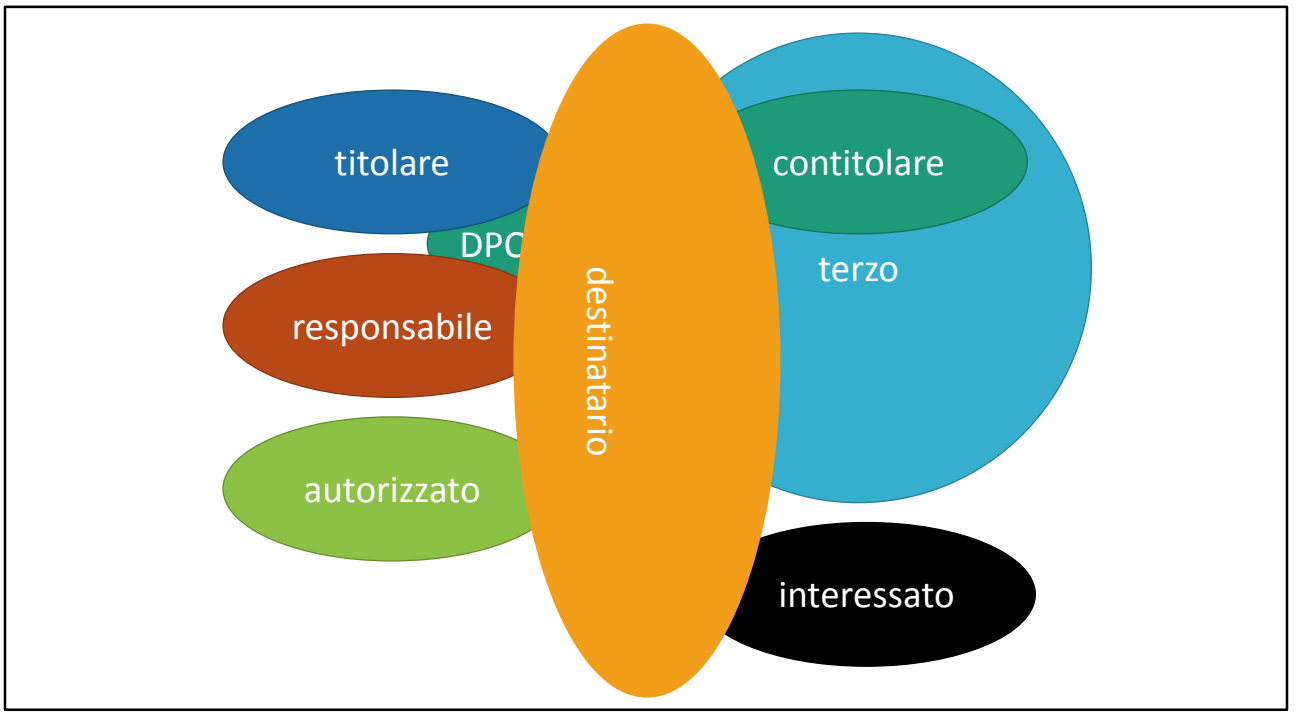
Le disposizioni del Codice in materia di incaricati del trattamento sono pienamente compatibili con la struttura e la filosofia del regolamento, in particolare alla luce del principio di "responsabilizzazione" di titolari e responsabili del trattamento che prevede l´adozione di misure atte a garantire proattivamente l´osservanza del regolamento nella sua interezza. In questo senso, titolari e responsabili del trattamento possono mantenere in essere la struttura organizzativa e le modalità di designazione degli incaricati di trattamento così come delineatesi negli anni anche attraverso gli interventi del Garante in quanto misure atte a garantire e dimostrare "che il trattamento è effettuato conformemente" al regolamento

Infatti, ai sensi dell'Art. 2-quaterdecies Nuovo Codice (dlgs. 101/2018) , relativo all'Attribuzione di funzioni e compiti a soggetti designati,
Il titolare o il responsabile del trattamento

- possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.
- individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.

Il considerando 29 in premessa al GDPR recita:
«Il titolare del trattamento che effettua il trattamento dei dati personali dovrebbe indicare le persone autorizzate all'interno dello stesso titolare del trattamento»

Pertanto la designazione formale delle persone autorizzate è da considerarsi una misura di sicurezza sempre adeguata!



In questa rappresentazione grafica degli insiemi sono mostrati i vari ruoli
Titolare
Responsabile
Con i loro DPO
Ed autorizzati

A destra gli interessati ed i terzi, tra cui i contitolari

Nel centro i destinatari nel cui novero possono rientrare tutti i ruoli

E' bene rilevare che la stessa persona fisica può ricoprire contemporaneamente più ruoli:
ad esempio un lavoratore è

- tanto un «interessato», visto che i suoi dati personali sono oggetto di trattamento da parte del datore di lavoro e probabilmente anche di qualche cliente o fornitore del proprio datore di lavoro quale referente o contatto in quale commessa, fornitura o progetto
- Quanto un «autorizzato», visto che presumibilmente tratterà i dati personali di clienti, fornitori, utenti o anche dei propri colleghi per

trattamenti riconducibili alla sua attività lavorativa che dipende dal suo datore di lavoro, nell'accezione più estesa, che sarà dunque titolare di quei trattamenti, soggetto all'applicazione del GDPR

Dunque questo corso vale sia come informazione e formazione in merito ai diritti degli interessati (che vedremo a breve), sia in merito ai principi, ai compiti, agli adempimenti e ad alcune misure di sicurezza che gli autorizzati devono conoscere ed applicare.

Principi applicabili & accountability

- Il titolare del trattamento deve essere in grado di comprovare il rispetto, che gli compete, di tutti i principi:

1. liceità, correttezza e trasparenza
2. limitazione della finalità
3. minimizzazione dei dati
4. esattezza
5. limitazione della conservazione
6. integrità e riservatezza

- Reg.(UE)2016/679 art. 5 co. 1 & 2

Principio di responsabilizzazione (accountability)

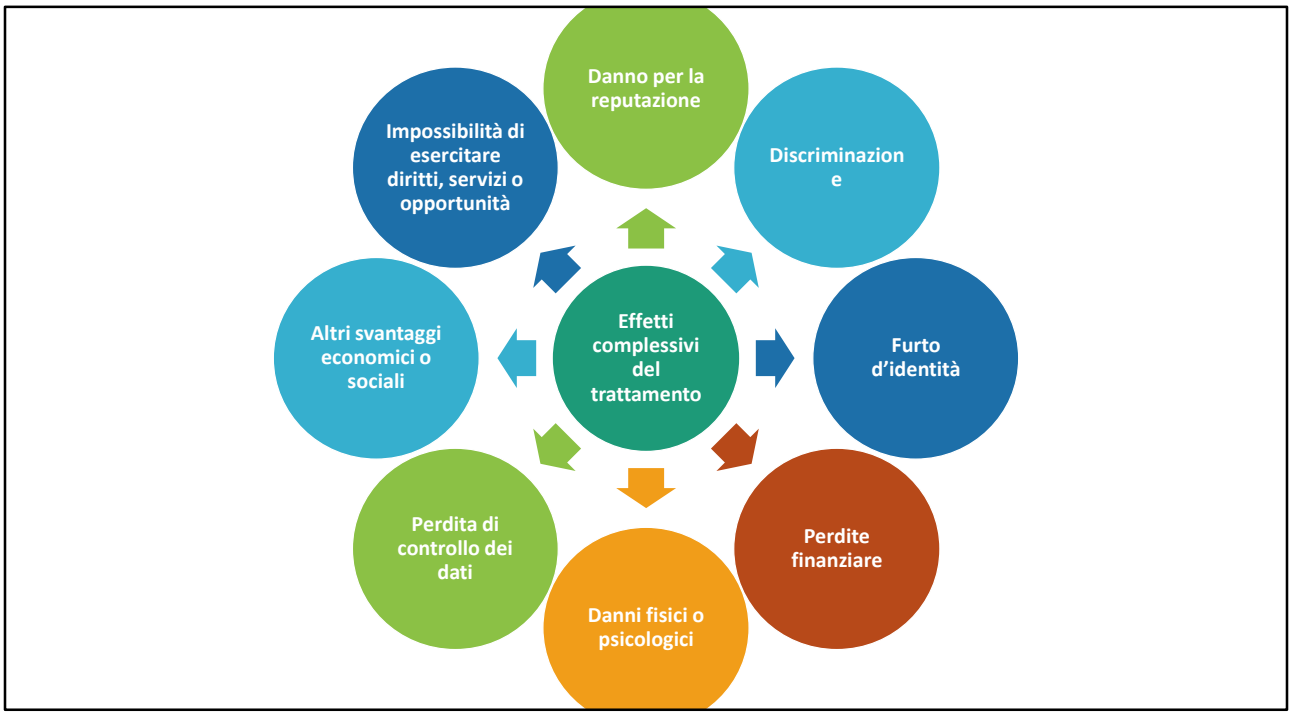
Secondo questo principio il titolare del trattamento deve essere in grado di comprovare il rispetto, che gli compete, di tutti i precedenti principi:

1. liceità, correttezza e trasparenza
2. limitazione della finalità
3. minimizzazione dei dati
4. esattezza
5. limitazione della conservazione
6. integrità e riservatezza

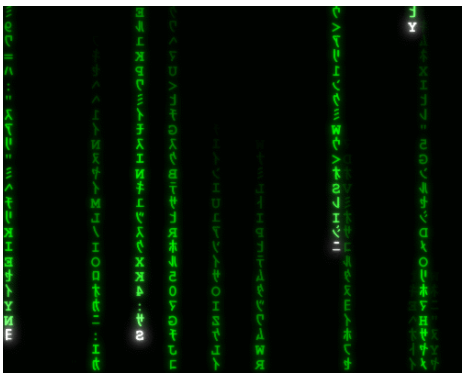
Tale responsabilizzazione comporta adozione di politiche privacy

- implementazione di misure tecniche e organizzative adeguate
- conservazione della documentazione di tutti i trattamenti
  - effettuati sotto la propria titolarità (e responsabilità),
  - indicando obbligatoriamente per ognuno di essi una serie nutrita di informazioni, tali da assicurare e comprovare la conformità di ciascuna operazione alle disposizioni del Regolamento (si veda quindi la necessità dei Registri delle attività di trattamento anche

ove non obbligatori!)


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

Diritti dell'interessato



Facciamo ora una carrellata dei diritti degli interessati
Tralasciando, per ora il tema, delle informative, come venivano indicate nel previgente Codice, cioè quelle informazioni che gli interessati devono obbligatoriamente ricevere dai titolari sia nel caso in cui la raccolta dei loro dati avvenga direttamente o indirettamente

Esistenza e Accesso

- L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano
- L'interessato ha diritto di ottenere l'accesso ai dati personali e alle informazioni presenti nell'informativa

- Reg.(UE)2016/679 art. 16

- Es. le finalità del trattamento; le categorie di dati personali in questione; i destinatari; il periodo di conservazione; i diritti dell'interessato
- Es. qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine; l'esistenza di un processo decisionale automatizzato, compresa la profilazione, nonché l'importanza e le conseguenze previste

Esistenza

L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano

Accesso

L'interessato ha diritto di ottenere l'accesso ai dati personali e alle informazioni presenti nell'informativa

Ad Es.
l'interessato ha diritto di conoscere le finalità del trattamento; le categorie di dati personali in questione; i destinatari; il periodo di conservazione; i diritti dell'interessato
Inoltre qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine; l'esistenza di un processo decisionale automatizzato, compresa la profilazione, nonché l'importanza e le conseguenze previste

Copia dei dati

- L'interessato ha diritto di ottenere la comunicazione in forma intelligibile dei dati personali che lo riguardano

Reg.(UE)2016/679 art. 16

- Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento.
  - In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi.

Copia dei dati

L'interessato ha diritto di ottenere la comunicazione in forma intelligibile dei dati personali che lo riguardano

Quindi il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento.

In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi.

Rettifica

- L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo.
- Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa

- Reg.(UE)2016/679 art. 16

Rettifica

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo.
Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa

Cancellazione (diritto all'oblio)

- L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo, se sussistono alcuni specifici motivi o ricorrono alcune condizioni.

- Reg.(UE)2016/679 art. 17

Cancellazione (diritto all'oblio)

L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo, se sussistono alcuni specifici motivi o ricorrono alcune condizioni.

In caso di Limitazione di trattamento

- I dati personali possono essere trattati solo:

1. per la conservazione,
2. per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria
3. per tutelare i diritti di un'altra persona fisica o giuridica
4. per motivi di interesse pubblico rilevante
5. In tutti gli altri casi, soltanto con il consenso dell'interessato

- Reg.(UE)2016/679 art. 18

In caso di Limitazione di trattamento

I dati personali possono essere trattati solo:

1. per la conservazione,
2. per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria
3. per tutelare i diritti di un'altra persona fisica o giuridica
4. per motivi di interesse pubblico rilevante
5. In tutti gli altri casi, soltanto con il consenso dell'interessato

Portabilità

Reg.(UE)2016/679 art. 20

- qualora:

1. il trattamento si basi sul consenso o su un contratto **e**
2. il trattamento sia effettuato con mezzi automatizzati

- l'interessato deve poter migrare, senza impedimenti, i dati personali che lo riguardano da un titolare del trattamento a un altro titolare del trattamento
  - mediante un formato strutturato, di uso comune e leggibile da dispositivo automatico,
  - eventualmente mediante trasmissione diretta, se tecnicamente fattibile

Portabilità

qualora:

1. il trattamento si basi sul consenso o su un contratto **e**
2. Contestualmente sia anche effettuato con mezzi automatizzati

l'interessato deve poter migrare, senza impedimenti, i dati personali che lo riguardano da un titolare del trattamento a un altro titolare del trattamento

- mediante un formato strutturato, di uso comune e leggibile da dispositivo automatico,
- eventualmente mediante trasmissione diretta, se tecnicamente fattibile

Opposizione

Reg.(UE)2016/679 art. 21

- L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano condotto sulla base di
  - Interesse pubblico o Esercizio di pubblici poteri
  - Legittimo interesse del titolare del trattamento
- Salvo che il titolare dimostri l'esistenza di motivi legittimi cogenti
  - per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure
  - per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria

Opposizione

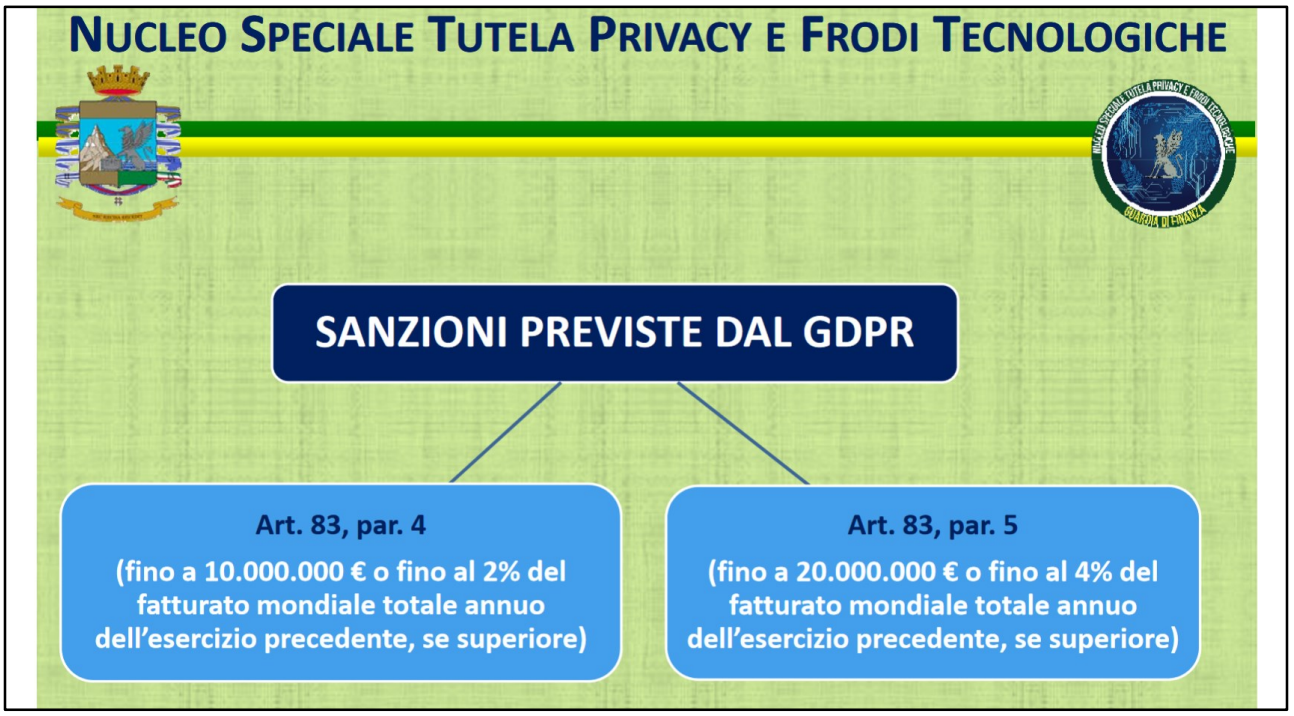
L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano condotto sulla base di

Interesse pubblico o Esercizio di pubblici poteri
Legittimo interesse del titolare del trattamento

Salvo che il titolare dimostri l'esistenza di motivi legittimi cogenti

per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure
per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria


NUCLEO SPECIALE TUTELA PRIVACY
E FRODI TECNOLOGICHE
DIPENDENZA GERARCHICA
UNITA' SPECIALI
AUTORITÀ DI RIFERIMENTO
GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI


NUCLEO SPECIALE TUTELA PRIVACY E FRODI TECNOLOGICHE
SANZIONI PREVISTE DAL GDPR
Art. 83, par. 4
(fino a 10.000.000 € o fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore)
Art. 83, par. 5
(fino a 20.000.000 € o fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore)

il GDPR fissa solo il massimo delle sanzioni **di natura amministrativa** in caso di violazioni della normativa sulla protezione dei dati personali.
Tali limiti sono di particolare rilevanza!

In particolare, l’art. 83 del GDPR distingue **due gruppi di sanzioni amministrative**: nel primo gruppo rientrano le **violazioni cosiddette di minore gravità**, per le quali sono previste le sanzioni amministrative pecuniarie di importi fino a 10 milioni di euro o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell’esercizio precedente, se superiore, e riguardano nello specifico le violazioni degli obblighi imposti ai seguenti soggetti:

- il titolare ed il responsabile del trattamento (artt. 8, 11, da 25 a 39, 42 e 43 GDPR);
- l’organismo di certificazione, Accredia;
- l’organismo di controllo dei codici di condotta (art. 41 GDPR);

Il **secondo gruppo di sanzioni**, più pesanti in considerazione della maggiore gravità delle fattispecie a cui sono ricondotte, ammontano fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo

dell'esercizio precedente, se superiore, e riguardano nello specifico le seguenti violazioni:

- dei principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9;
- dei diritti degli interessati a norma degli articoli da 12 a 22;
- i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49;
- qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX;
- l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati del Garante ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1 GDPR.

Nell'adeguamento del Codice Privacy nazionale, il d.lgs. 101/2018 ha apportato rilevanti modifiche, prevedendo ulteriori fattispecie di illeciti soggetti alle predette sanzioni amministrative, ma non ci soffermeremo su di esse.

Oltre alla sanzione pecuniaria, potrà essere applicata anche quella accessoria della pubblicazione dell'ordinanza-ingiunzione, per intero o per estratto, sul sito internet del Garante.

E' tuttavia ammesso un pagamento della sanzione in forma ridotta: Entro 30 giorni dalla data di comunicazione del provvedimento sanzionatorio, il trasgressore e gli obbligati in solido possono definire la controversia adeguandosi alle prescrizioni del Garante, ove impartite, e mediante il pagamento di un importo pari alla metà della sanzione irrogata

A corredo di quanto sopra, vale la pena sottolineare che I proventi delle sanzioni, nella misura del 50% per cento del totale annuo, sono destinati alle specifiche attività di sensibilizzazione e di ispezione nonché di attuazione del Regolamento svolte dal Garante

Illeciti Penali

d.lgs.196/2003

Art.	Tipologia	Sanzione
167 co.1	Trattamento Illecito dei dati – e-privacy	Reclusione 6-18 mesi
167 co.2	Trattamento Illecito dei dati – dati particolari o relativi a condanne	Reclusione 12-36 mesi
167 co.3	Trattamento Illecito dei dati – trasferimenti extra-UE	Reclusione 12-36 mesi
167-bis	Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala	Reclusione 12-72 mesi
167-ter	Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala	Reclusione 12-48 mesi
168 co.1	Falsità in dichiarazioni al Garante	Reclusione 6-36 mesi
168 co.2	Interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante	Reclusione 0-12 mesi
170	Inosservanza di provvedimenti del Garante	Reclusione 3-24 mesi

Sanzioni derivanti da illecito penale

Con riguardo alle **sanzioni penali**, se da un lato il GDPR non ne prevede direttamente, lo stesso ammette dall'altro lato la facoltà per gli Stati membri di stabilire disposizioni relative a sanzioni penali per violazioni del GDPR, nonché violazioni di norme nazionali adottate in virtù ed entro i limiti del Regolamento.

Anche in questo caso è intervenuto il Decreto, modificando le fattispecie penalmente rilevanti già previste dal Codice Privacy ed integrando le stesse con ulteriori violazioni

Le fattispecie per cui saranno applicabili sanzioni penali per dolo specifico (per trarre profitto o arrecare danno) sono quindi, ai sensi del riformato Codice Privacy:
167 (**Trattamento illecito dei dati**)
167-bis (**Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala**);
167-ter (**Acquisizione fraudolenta di dati personali oggetto di trattamento su**

larga scala);
168 (**Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante**);
170 (**Inosservanza dei provvedimenti del Garante**);
Con pene di reclusione variabili

Per ottemperare all'indicazione del GDPR secondo cui l'imposizione di sanzioni penali per violazioni delle norme nazionali e di sanzioni amministrative **non** dovrebbe essere **in contrasto con il principio del *ne bis in idem*** quale interpretato dalla Corte di giustizia europea, il nuovo codice privacy prevede che
Quando per lo stesso fatto è stata applicata a norma del Codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa è stata riscossa, la pena è diminuita.


ORGANIZZAZIONE

Adempimenti vs. interessati

Rendere informativa

Gestire eventuale consenso/opposizione (OPT-IN vs. OPT-OUT)

Rispondere alle richieste di esercizio dei diritti

Effettuare le comunicazioni necessarie/opportune in caso di data breach

Adempimenti vs. garante

COMUNICAZIONE DEI DATI DEL DPO

NOTIFICAZIONE IN CASO DI DATA BREACH

CONSULTAZIONE PRELIMINARE

RISPOSTA ALLE RICHIESTE E LEALE COLLABORAZIONE

Adempimenti organizzativi (1)

autorizzazioni al trattamento

designazioni dei responsabili del trattamento e/o contitolari con eventuali trasferimenti extra ue

registri delle attività di trattamento (reat)

valutazione di impatto (dpia)

Adempimenti organizzativi (2)

Procedure di privacy by-design/default,

Misure di sicurezza

procedure per gestire gli altri adempimenti (es. vs. interessati/garante, cancellazione/conservazione dei dati)

Certificazioni e codici di condotta

Il «gioco» della privacy

.. una metafora applicativa

Dopo questa lunga panoramica introduttiva in cui, in ultimo, ci siamo soffermati sulla figura dell'interessato, che riguarda tutti noi, e sui suoi diritti, passiamo a considerare quanto riguarda i soggetti che svolgono il trattamento dei dati.
Se volessimo adottare una metafora, potremmo considerare questi soggetti come pedine di una specie di «gioco dell'oca» che chiameremmo quindi «gioco della privacy» in cui le caselle si susseguono così:

- Definire il trattamento (liceità, finalità, durata, ecc.)
- Scegliere e Garantire il presupposto di legittimità, cioè la base giuridica
- Rendere l'informativa all'interessato
- Se necessario, acquisire il consenso
- Adottare le misure di protezione e sicurezza (tecniche ed organizzative)
- Rispettare e Documentare gli adempimenti (designazioni, registri, valutazioni dei rischi, notifiche e comunicazioni)
- Dare eventuale riscontro agli interessati
- Mantenere aggiornati misure ed adempimenti
- Cancellare i dati al termine del periodo di conservazione

Passiamo dunque ad elencare i principi fondamentali a cui deve sottostare

ogni trattamento di dati personali

Quale presupposto di legittimità?

Liceità del trattamento

Liceità del trattamento

Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle condizioni (presupposti) di legittimità, cioè quando la base giuridica del trattamento è tra quelle ammesse dal GDPR.

Tutte queste basi hanno pari dignità e rilevanza. Tra queste ricorre ancora il consenso, ma differentemente a prima non è più l'elemento cardine.

1. Oltre al consenso esplicito dell'interessato per una o più specifiche finalità , il trattamento si può basare su
2. Obblighi contrattuali e precontrattuali (quanto il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso)
3. Obbligo legale (quando il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento)
4. Salvaguardia degli interessi vitali (quando il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica)
5. Interesse pubblico o Esercizio di pubblici poteri (quando il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso

all'esercizio di pubblici poteri di cui è investito il titolare del trattamento)
6. Archiviazione nel pubblico interesse, ricerca scientifica o storica o fini statistici
7. Legittimo interesse (quando il trattamento, purché non sia effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti, è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore)

Ad es. Costituisce legittimo interesse del titolare del trattamento interessato trattare dati personali relativi al traffico, in misura strettamente necessaria e proporzionata per garantire la sicurezza delle reti e dell'informazione

Divieto di trattare le categorie particolari di dati personali (sensibili, genetici, biometrici)

Vige il divieto di trattare le categorie particolari di dati personali (quelli cioè definiti sensibili, secondo il «vecchio» Codice, quelli genetici e biometrici) ammenoché non ricorrano le seguenti deroghe:

1. Consenso esplicito (salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto)
2. Obblighi giuslavoristici e di protezione sociale (quando il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo)
3. Organismi senza scopo di lucro che perseguono finalità politiche, filosofiche, religiose o sindacali (quando il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o

l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato)

4. Tutela di un interesse vitale (quando il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso)
5. Dati pubblici (quando il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato)
6. Difesa di un diritto in sede giudiziaria (quando il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali)
7. Esercizio di un diritto in sede giudiziaria
8. Rilevante interesse pubblico (quando il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri,
9. che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato)
10. Medicina e valutazione della capacità lavorativa (quando il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale)
11. Sanità pubblica (quando il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici)

Trasferimenti di dati verso paesi terzi o organizzazioni internazionale

- Il trasferimento verso un paese terzo o un'organizzazione internazionale di dati personali destinati a essere oggetto di un trattamento dopo il trasferimento può avere luogo

1. sulla base di una decisione di adeguatezza della Commissione UE
2. se sussistono garanzie adeguate quali, tra l'altro,
   a) Norme vincolanti d'impresa
   b) Clausole contrattuali tipo

https://www.cnil.fr/en/data-protection-around-the-world

- Reg.(UE)2016/679 art. 44

Ulteriori rilevanti adempimenti riguardano i Trasferimenti di dati extra Unione, verso paesi terzi o organizzazioni internazionale.

Il regolamento ha confermato l´approccio attualmente vigente per quanto riguarda i flussi di dati al di fuori dell´Unione europea e dello spazio economico europeo, prevedendo che tali flussi sono vietati, in linea di principio, a meno che intervengano specifiche garanzie che il regolamento elenca in ordine gerarchico:

1) adeguatezza del Paese terzo riconosciuta tramite decisione della Commissione europea;
2) in assenza di decisioni di adeguatezza della Commissione, garanzie adeguate di natura contrattuale o pattizia che devono essere fornite dai titolari coinvolti (fra cui le norme vincolanti d´impresa - BCR, e clausole contrattuali tipo);
3) in assenza di ogni altro presupposto, utilizzo di deroghe al divieto di trasferimento applicabili in specifiche situazioni.

Viene dunque meno il requisito dell´autorizzazione nazionale. Ma le

decisioni di adeguatezza sinora adottate dalla Commissione (livello di protezione dati in Paesi terzi, a partire dal Privacy Shield USA, e clausole contrattuali tipo per titolari e responsabili) e gli accordi internazionali in materia di trasferimento dati stipulati prima del 24 maggio 2016 dagli Stati membri restano in vigore fino a loro eventuale revisione o modifica. Restano valide, conseguentemente, le autorizzazioni nazionali sinora emesse dal Garante successivamente a tali decisioni di adeguatezza della Commissione. Restano valide, inoltre, le autorizzazioni nazionali che il Garante ha rilasciato in questi anni per specifici casi, sino a loro eventuale modifica.

Tuttavia, **l´autorizzazione del Garante sarà ancora necessaria** se un titolare desidera utilizzare **clausole contrattuali ad-hoc** (cioè non riconosciute come adeguate tramite decisione della Commissione europea) oppure **accordi amministrativi** stipulati tra autorità pubbliche – una delle novità introdotte dal regolamento.

Ad esempio Il regolamento vieta trasferimenti di dati verso titolari o responsabili in un Paese terzo sulla base di **decisioni giudiziarie o ordinanze amministrative emesse da autorità di tale Paese terzo**, a meno dell´esistenza di accordi internazionali in particolare di mutua assistenza giudiziaria o analoghi accordi fra gli Stati *(si veda art. 48)*. Si potranno utilizzare, tuttavia, gli altri presupposti e in particolare le deroghe previste per situazioni specifiche di cui all´art. 49. A tale riguardo, si deve ricordare che il regolamento chiarisce come sia lecito trasferire dati personali verso un Paese terzo non adeguato "per importanti motivi di interesse pubblico", in deroga al divieto generale, ma deve trattarsi di un **interesse pubblico riconosciuto dal diritto dello Stato membro** del titolare o dal diritto dell´Ue – e dunque non può essere fatto valere l´interesse pubblico dello Stato terzo ricevente.

Privacy by design

Reg.(UE)2016/679 art. 25

fin dalla progettazione,
il titolare del trattamento mette in atto misure tecniche e organizzative adeguate volte a

1. attuare in modo efficace i principi di protezione dei dati (es. Minimizzazione)
2. a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati

   - 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

Privacy by design

fin dalla progettazione, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate volte a

1. attuare in modo efficace i principi di protezione dei dati (es. Minimizzazione)
2. a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati

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

Privacy by default

Reg.(UE)2016/679 art. 25

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire

1. che siano trattati, **per impostazione predefinita**, solo i dati personali necessari per ogni specifica finalità del trattamento
   Tale obbligo vale per
   - la quantità dei dati personali raccolti,
   - la portata del trattamento,
   - il periodo di conservazione e
   - l'accessibilità
2. che non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica

Privacy by default

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire

1. che siano trattati, **per impostazione predefinita**, solo i dati personali necessari per ogni specifica finalità del trattamento
   Tale obbligo vale per
   la quantità dei dati personali raccolti,
   la portata del trattamento,
   il periodo di conservazione e
   l'accessibilità
2. che non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica

Rendere l'informativa all'interessato

Informativa

non si applica se e nella misura in cui l'interessato dispone già di tutte le informazioni previste

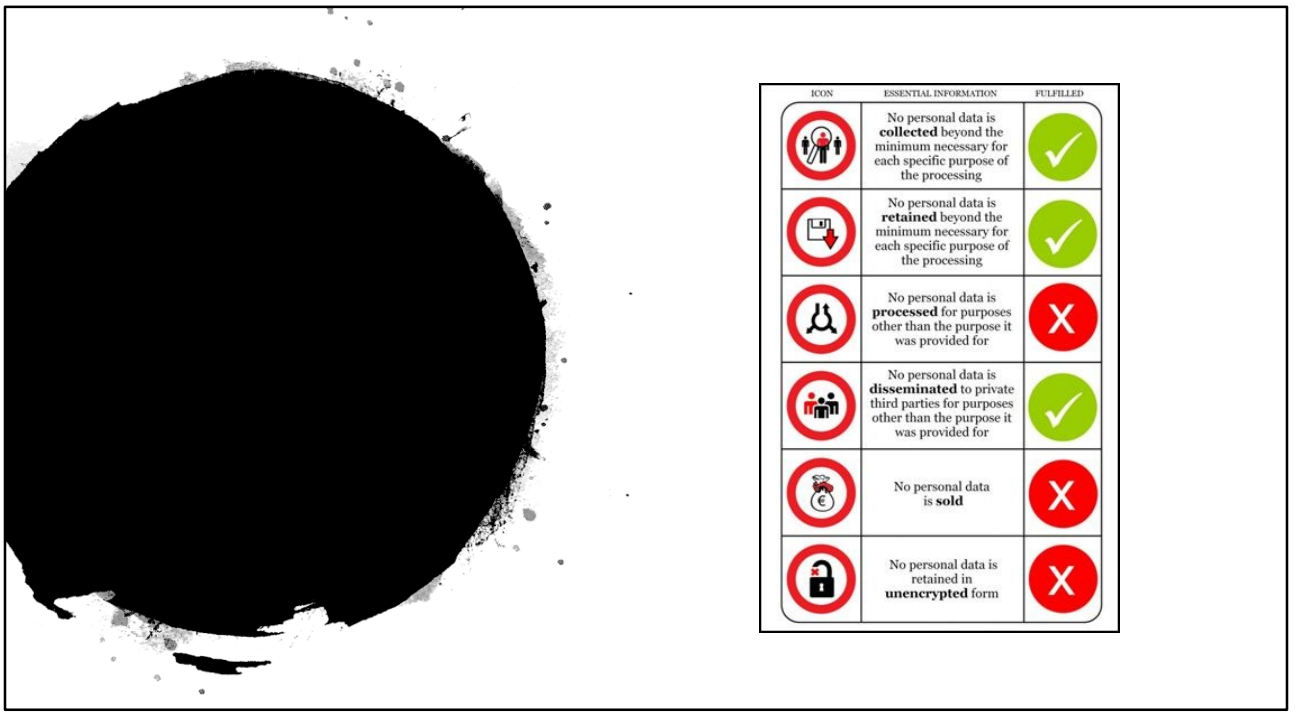
L'obbligo di rendere l'informativa (informazioni ai sensi degli articoli 13 e 14 del GDPR) non si applica se e nella misura in cui l'interessato dispone già di tutte le informazioni previste.

l'informativa è necessaria:

- In caso di raccolta presso l'interessato
- Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella originaria
- Qualora i dati non siano stati ottenuti presso l'interessato

In quest'ultimo caso, quando i dati non sono stati ottenuti presso l'interessato, l'informativa va resa

1. O entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese
2. O, nel caso in cui i dati personali siano destinati alla comunicazione (con l'interessato o ad altro destinatario), al più tardi al momento della prima comunicazione (quindi non necessariamente all'atto della registrazione !!)



I contenuti dell'informativa sono:

- l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante
- i dati di contatto del responsabile della protezione dei dati, ove applicabile
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento
- L'indicazione dei legittimi interessi perseguiti, se pertinenti
- le categorie di dati personali in questione, solo qualora i dati non siano stati ottenuti presso 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 qualora i dati non siano stati ottenuti presso l'interessato
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali
- se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati, solo qualora i dati

siano stati raccolti ed ottenuti presso l'interessato

- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione , in tal caso, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato
- ove applicabile,

1. l'intenzione del titolare del trattamento di trasferire dati personali a un destinatario in un paese terzo o a un'organizzazione internazionale e
2. l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.

- l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati
- il diritto di proporre reclamo a un'autorità di controllo
- l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca, solo qualora il trattamento sia basato sul consenso esplicito dell’interessato

Misure di sicurezza

Reg.(UE)2016/679 art. 32

- Pseudonimizzazione
- Cifratura dei dati personali
- Capacità di assicurare su base permanente **la riservatezza, l'integrità, la disponibilità** e la resilienza dei sistemi e dei servizi di trattamento
- 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

Il GDPR diversamente dal previgente Codice non impone un livello minimo di misure di sicurezza, ma fornisce alcune indicazioni in merito alle misure di sicurezza da adottarsi, sulla base della valutazione dei rischi (o quella generalizzata ai sensi dell'art.32, o quella di impatto ai sensi dell'art.35, o addirittura quella che coinvolge il Garante ai sensi dell'art.36)

Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento;
Per lo stesso motivo, **non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza** *(art. 33 del «vecchio» Codice)* poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da art. 32 del regolamento.

In questo senso, il GDPR con **la lista di cui al paragrafo 1 dell´art. 32 propone una lista aperta e non esaustiva**
queste misure esplicitamente indicate, ma non necessariamente obbligatorie comprendono:

- Pseudonimizzazione

- Cifratura dei dati personali
- Capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento
- 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

In ogni caso, un punto di partenza sono le misure dettagliate nel Allegato B del «vecchio» Codice, ora abrogato, il quale imponeva l'adozione di:

- procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti
- procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati
- Utilizzazione di un sistema autenticazione informatica;
- Adozione di procedure di gestione delle credenziali di autenticazione
- Utilizzazione di un sistema di autorizzazione
- Protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici
- Adozione di procedure per la custodia di copie di sicurezza (back-up), il ripristino della disponibilità dei dati e dei sistemi
- Aggiornamento periodico di sistemi operativi, software di protezione e di trattamento
- Formazione ed informazione periodica degli incaricati/responsabili

Si richiama l´attenzione anche sulla possibilità di utilizzare l´adesione a specifici codici di condotta o a schemi di certificazione per attestare l´adeguatezza delle misure di sicurezza adottate.
Tuttavia, l´Autorità potrà valutare la definizione di linee-guida o buone prassi sulla base dei risultati positivi conseguiti in questi anni; inoltre, per alcune tipologie di trattamenti (quelli di cui all´art. 6, paragrafo 1), lettere c) ed e) del regolamento) potranno restare in vigore (in base all´art. 6, paragrafo 2, del regolamento) le misure di sicurezza attualmente previste attraverso le disposizioni di legge volta per volta applicabili: è il caso, in particolare, dei trattamenti di dati sensibili svolti dai soggetti pubblici per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22 Codice), ove questi ultimi contengano disposizioni in materia di sicurezza dei trattamenti.

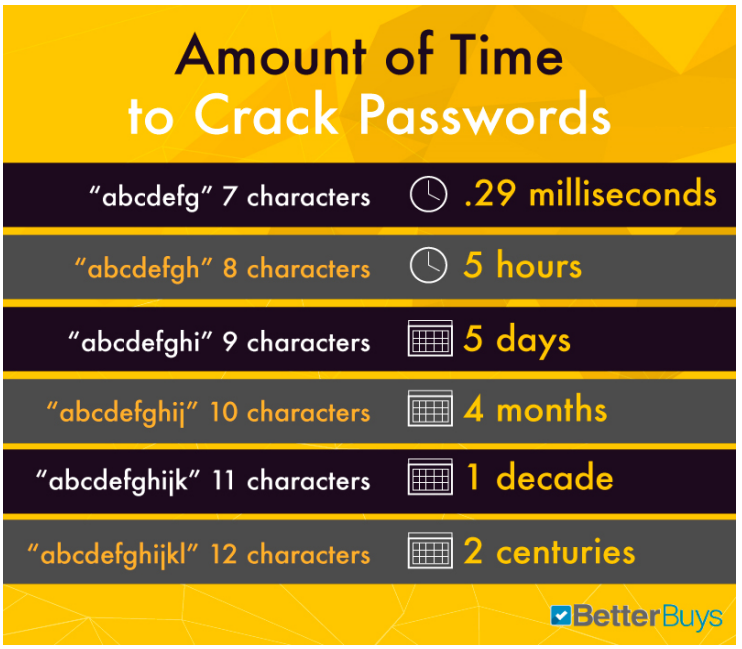
QUALI SONO LE MISURE PER LA GESTIONE DEL RISCHIO? **ACCOUNTABILITY**

Misure di sicurezza (2)

d.lgs.196/2003 artt. 33-36 Allegato B

Nel caso di utilizzo di strumentazione elettronica:

- Utilizzazione di un sistema autenticazione informatica;
- Adozione di procedure di gestione delle credenziali di autenticazione
- Utilizzazione di un sistema di autorizzazione
- Protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici
- Adozione di procedure per la custodia di copie di sicurezza (back-up), il ripristino della disponibilità dei dati e dei sistemi
- Aggiornamento periodico di sistemi operativi, software di protezione e di trattamento


Amount of Time
to Crack Passwords
"abcdefg" 7 characters
.29 milliseconds
"abcdefgh" 8 characters
5 hours
"abcdefghi" 9 characters
5 days
"abcdefghij" 10 characters
4 months
"abcdefghijk" 11 characters
1 decade
"abcdefghijkl" 12 characters
2 centuries
BetterBuys

Password: buone prassi

- Scegliere una password lunga (almeno 8 caratteri);
- Renderla complessa, evitando parole presenti nel vocabolario o sequenze di numeri facili da individuare da parte di un umano o di un software;
- Inserire sempre un mix di numeri, lettere maiuscole e minuscole, eventualmente segni di punteggiatura;
- Usare password diverse per l'accesso a servizi diversi;
- Scegliere password che si possano ricordare
  - magari una “passphrase”, una frase facile da ricordare ma “complicata” da acronimi, numeri e maiuscole
- Cambiare periodicamente la password ogni 3 mesi per i dati «rilevanti» e ogni 6 mesi negli altri casi

Password: errori più comuni da evitare

- Usare una parte qualsiasi del proprio nome
- Il nome del proprio account, ovvero il cosiddetto UserID (identificativo utente).
- Una parola con meno di 7 caratteri
- Una parte qualsiasi del nome di un membro della propria famiglia (animali domestici inclusi) o, peggio, quello di un collega
- Nomi di sistemi operativi
- Numeri con significati particolari (ad esempio, numeri di telefono e targhe automobilistiche)
- Nomi di luoghi
- Cose preferite o più detestate
- Facili associazioni con cose preferite o detestate: per esempio, "Aragorn" è una password pessima per un fan de "Il Signore degli Anelli"
- Una qualsiasi parola dalla corretta grammatica, in inglese come nella propria lingua madre, specialmente quelle che con ogni probabilità sono incluse in dizionari di parole d'uso comune. Ad esempio, "il mio nome" è una password non idonea per chi parla italiano

Misure di sicurezza (3)

d.lgs.196/2003 artt. 33-36 Allegato B

- **Definizione dei compiti e dell'ambito del trattamento consentito**
- Previsione di **procedure per un'idonea custodia** di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti
- Previsione di **procedure per la conservazione** di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati

Almeno una volta all'anno:

- Effettuazione dell'**analisi dei rischi** di distruzione o perdita dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta
- **Aggiornamento dell'individuazione dell'ambito del trattamento consentito** ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
- **Formazione ed informazione** degli incaricati/responsabili

Formazione e Istruzioni obbligatorie

Reg.(UE)2016/679
art. 29, art. 32 co.4

- Chiunque (incaricato o responsabile) abbia accesso ai dati deve essere istruito al riguardo da parte del titolare del trattamento

Per l'appunto il GDPR stabilisce che Chiunque (incaricato o responsabile) abbia accesso ai dati debba essere istruito (e formato) al riguardo da parte del titolare del trattamento

Contratto di responsabilità

Reg.(UE)2016/679 art. 28 co.3, 9

- è stipulato in forma scritta, anche in formato elettronico
- prevede, in particolare, alcuni obblighi per il responsabile del trattamento

Contratto di responsabilità

Il GDPR entra nel merito della forma e del contenuto del Contratto in cui il titolare designa un responsabile

Questo è stipulato in forma scritta, anche in formato elettronico
Deve prevede, in particolare, che il responsabile del trattamento:

1. tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo
2. garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza
3. adotti tutte le misure di sicurezza richieste (articolo 32)
4. rispetti le condizioni per ricorrere a un altro responsabile del trattamento (subdelega)
5. assista il titolare del trattamento per dare seguito alle richieste per l'esercizio dei diritti dell'interessato
6. assista il titolare del trattamento nel garantire il rispetto degli obblighi

(articoli da 32 a 36) di sicurezza, di valutazione di impatto e in caso di violazioni

7. su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo non sia prevista per Legge la conservazione dei dati
8. metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi che gli competono
9. consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato
10. provveda ad informare immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi una norma di legge relativa alla protezione dei dati.

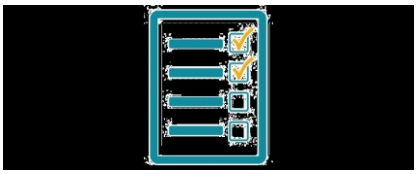
L’organizzazione deve:

- Nominare i propri fornitori / collaboratori esterni
- Farsi nominare dai propri clienti nei casi previsti
  - cfr. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9080970

Tenuta dei Registri delle attività di trattamento

Reg.(UE)2016/679 art. 30

- Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte.
- Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento



Tenuta dei Registri delle attività di trattamento

Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio, devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all´art. 30. In particolare Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento

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.

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, il Garante invita 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.

Valutazione di impatto (DPIA=Data Protection Impact Assessment)

Reg.(UE)2016/679 art. 35

il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali

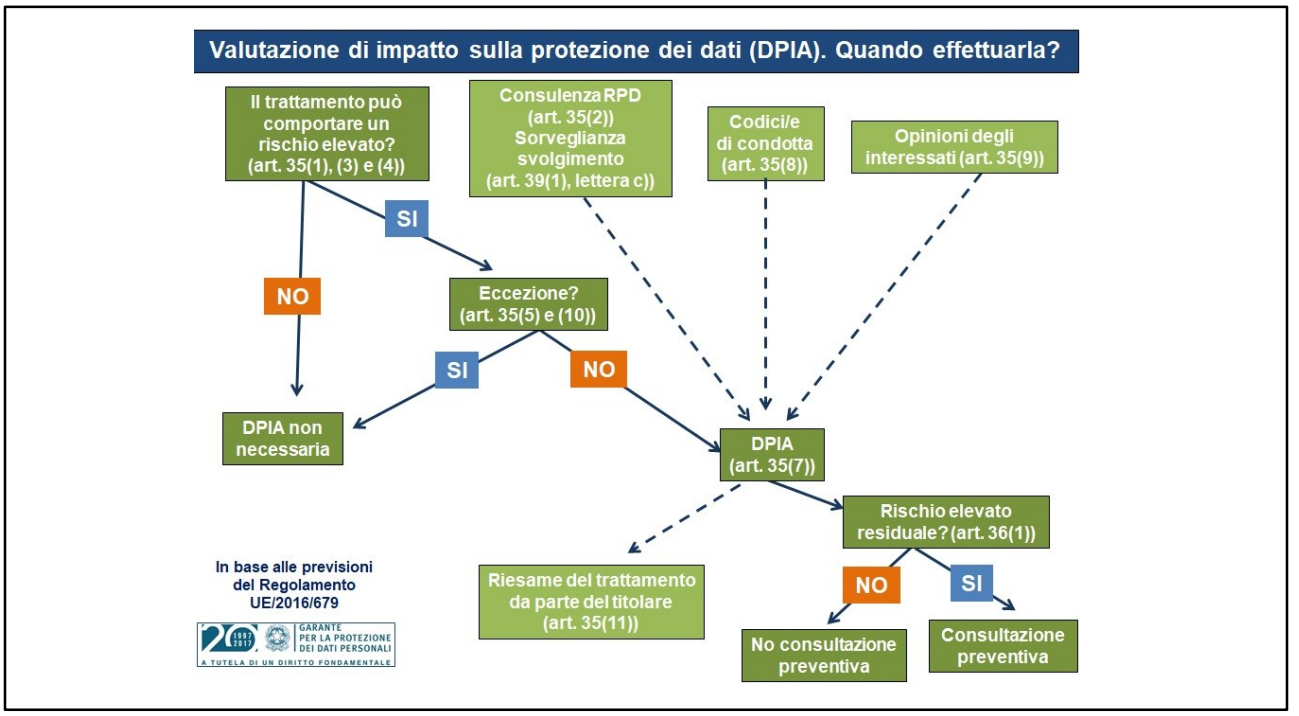
1. In generale, quando il trattamento può presentare un **rischio elevato** per i diritti e le libertà delle persone fisiche, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento
2. In particolare, obbligatoria in taluni casi (…)
3. Salvo i casi in cui ciò non sia esplicitamente escluso (…)

Valutazione di impatto

In alcuni casi particolari,
il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali

Tale valutazione, detta in inglese Data Protection Impact Assessment o con l'acronimo DPIA, è un approfondimento di quella generalizzata

E' necessaria, in generale, quando il trattamento può presentare un **rischio elevato** per i diritti e le libertà delle persone fisiche, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento



Quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate (a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono magari trattati dati sensibili, o anche per una combinazione di questi e altri fattori), il GDPR obbliga i titolari a svolgere una valutazione di impatto prima di darvi inizio, consultando l´autorità di controllo in caso le misure tecniche e organizzative da loro stessi individuate per mitigare l´impatto del trattamento non siano ritenute sufficienti - cioè, quando il rischio residuale per i diritti e le libertà degli interessati resti elevato.

Si tratta di uno degli elementi di maggiore rilevanza nel nuovo quadro normativo, perché esprime chiaramente la responsabilizzazione (accountability) dei titolari nei confronti dei trattamenti da questi effettuati. I titolari sono infatti tenuti non soltanto a garantire l´osservanza delle disposizioni del regolamento, ma anche a dimostrare adeguatamente in che modo garantiscono tale osservanza; la valutazione di impatto ne è un esempio.

Le linee-guida del Working Party 29 offrono alcuni chiarimenti sul punto; in

particolare, precisano quando una valutazione di impatto sia obbligatoria (oltre ai casi espressamente indicati dal regolamento all´art. 35), chi debba condurla (il titolare, coadiuvato dal responsabile della protezione dei dati, se designato), in cosa essa consista (fornendo alcuni esempi basati su schemi già collaudati in alcuni settori), e la necessità di interpretarla come un processo soggetto a revisione continua piuttosto che come un adempimento una tantum.

La **responsabilità** della DPIA spetta al **titolare**, anche se la conduzione materiale della valutazione di impatto può essere affidata a un altro soggetto, interno o esterno all'organizzazione. Il titolare **ne monitora** lo svolgimento **consultandosi** con il **responsabile della protezione dei dati** (RPD, in inglese DPO) e acquisendo - se i trattamenti lo richiedono - il parere di esperti di settore, del **responsabile della sicurezza dei sistemi informativi** (Chief Information Security Officer, CISO) e **del responsabile IT**.

La DPIA deve essere condotta **prima** di procedere al trattamento. Dovrebbe comunque essere previsto un **riesame continuo** della DPIA, **ripetendo la valutazione a intervalli regolari.**

Situazioni in cui vige l'obbligo della Valutazione di impatto

Reg.(UE)2016/679 art. 35 co.3/4

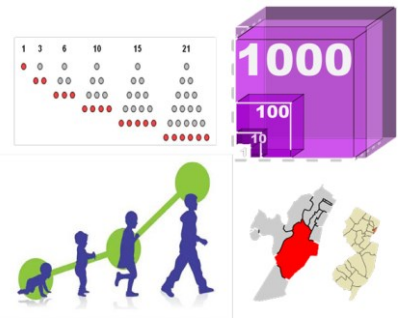
1. valutazione **sistematica e globale** di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche
2. trattamento, **su larga scala**, di categorie particolari di dati personali (sensibili, genetici, biometrici identificativi) o di dati relativi a condanne penali e a reati (giudiziari)
3. la sorveglianza sistematica **su larga scala** di una zona accessibile al pubblico.
4. per le tipologie di trattamenti inserite negli elenchi predisposti dalle autorità di controllo

Cosa si intende per «larga scala»? (1)

- Inizialmente negli atti del Parlamento Europeo, un trattamento si considerava su «larga scala» se riguardava non meno di 5 000 interessati durante qualsiasi periodo di 12 mesi consecutivi
- **Un'indicazione quantitativa certa, al momento, non c'è!**

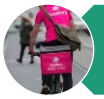
Cosa si intende per «larga scala»? (2)

- **<u>Esiste una linea guida del 13/12/2016 del WP29:</u>** si deve tenere conto di:
  - il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
  - il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
  - la durata, ovvero la persistenza, dell'attività di trattamento;
  - la portata geografica dell'attività di trattamento



Esempi di trattamenti su «larga scala»

trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati



trattamento di dati di geolocalizzazione raccolti in tempo reale per finalità statistiche da un responsabile specializzato nella prestazione di servizi di questo tipo rispetto ai clienti di una catena internazionale di fast food;

trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività

trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale;

trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (per esempio, il loro tracciamento attraverso titoli di viaggio)

trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici.

trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o di una banca nell'ambito delle ordinarie attività;

sorveglianza svolta da un'impresa di sicurezza privata relativa a più centri commerciali e aree pubbliche

Non è su «larga scala»:

trattamento di dati relativi a pazienti svolto da un singolo professionista sanitario

trattamento di dati personali relativi a condanne penali e reati svolto da un singolo avvocato

trattamento di dati personali relativi a contribuenti svolto da un singolo fiscalista

Documentazione in merito alla violazione dei dati personali

Reg.(UE)2016/679 art. 33

Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese:

1. le circostanze a essa relative
   - natura, categorie e numero approssimativo di interessati
2. le conseguenze probabili
3. i provvedimenti adottati e da adottare per porvi rimedio
4. il rischio per i diritti e le libertà delle persone fisiche
   - su cui si basano i due successivi adempimenti

Documentazione in merito alla violazione dei dati personali

Tutti i titolari di trattamento devono in ogni caso **documentare le violazioni** di dati personali subite, anche se non notificate all´autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati

tale obbligo non è diverso, nella sostanza, da quello previsto dall´art. 32-bis, comma 7, del «vecchio» Codice.

Il Garante raccomanda, pertanto, ai titolari di trattamento di adottare le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuti a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

I dati da registrare in merito ad una violazione di dati personali comprendono:

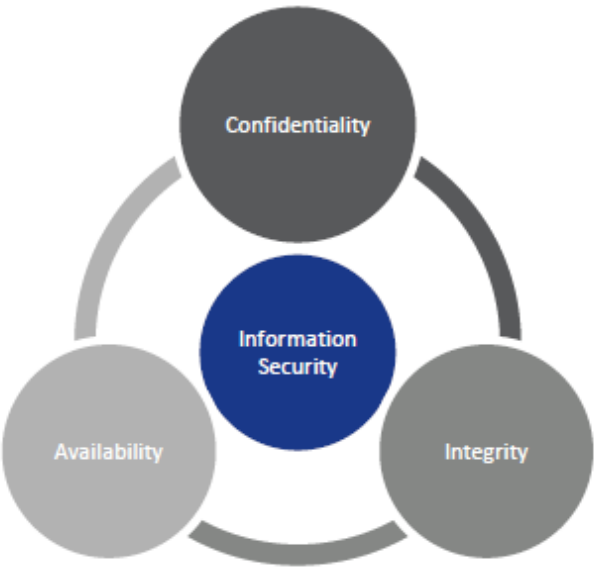
1. le circostanze a essa relative
   natura, categorie e numero approssimativo di interessati

2. le conseguenze probabili
3. i provvedimenti adottati e da adottare per porvi rimedio
4. il rischio per i diritti e le libertà delle persone fisiche

su cui si basano i due successivi adempimenti

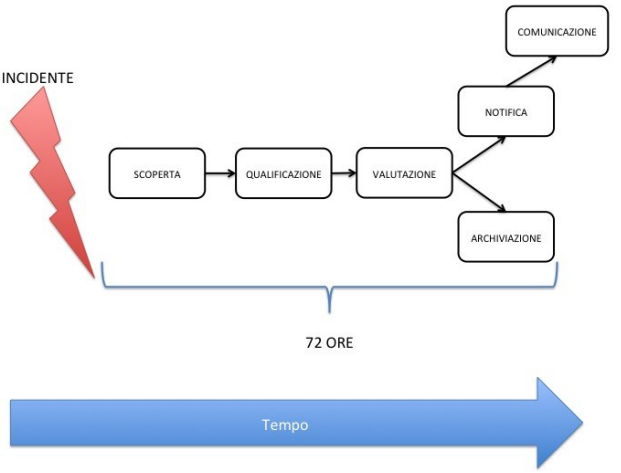
Hai subito un databreach dei tuoi dati?

https://monitor.firefox.com/



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

- In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente
  - 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
- Reg.(UE)2016/679 art. 33



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

A partire dal 25 maggio 2018, **tutti i titolari** – e non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avviene oggi – dovranno notificare all´autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, **entro 72 ore** e comunque "senza ingiustificato ritardo", ma **soltanto se ritengono probabile che da tale violazione derivino rischi** per i diritti e le libertà degli interessati.

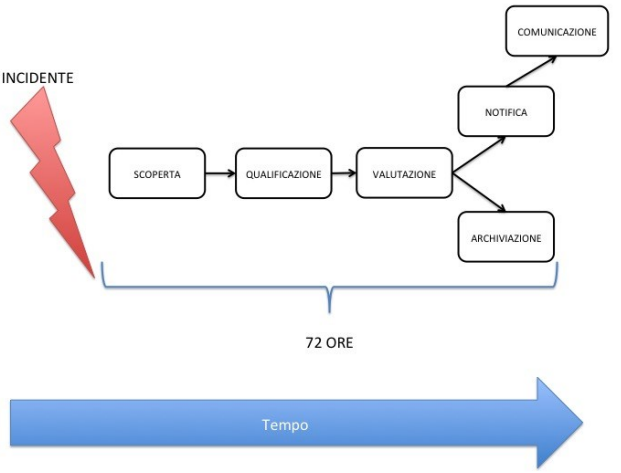
Pertanto, **la notifica all´autorità** dell´avvenuta violazione **non è obbligatoria**, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al titolare.

Comunque tutte le persone autorizzate ed anche i responsabili devono concorrere all'applicazione di tale obbligo coinvolgendo tempestivamente il Titolare in caso di violazioni rilevate così da poterle qualificare, valutare e prendere gli opportuni provvedimenti.

Comunicazione di una violazione dei dati personali all'interessato

- 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
  - Salvo che i dati non fossero cifrati, ecc.

- Reg.(UE)2016/679 art. 34



Comunicazione di una violazione dei dati personali all'interessato

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, oltre alla notificazione al Garante, comunica la violazione all'interessato senza ingiustificato ritardo

fanno eccezione le circostanze indicate al paragrafo 3 dell´art. 34 del GDPR, tra cui la cifratura dei dati

Gli adempimenti della notificazione e della comunicazione erano già previsti nel vecchio Codice, ma si applicavano limitatamente ai l fornitore di servizi di comunicazione elettronica accessibili al pubblico

Riesame ed aggiornamento

- Le misure **Reg.(UE)2016/679 art. 24**
  - tecniche e organizzative
  - adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento
- sono riesaminate e aggiornate qualora necessario

Reg.(UE)2016/679 art. 35 co.11

- Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento

Riesame ed aggiornamento

Tutti gli adempimenti descritti:

- Politiche adeguate
- Privacy by design
- Privacy by default
- Valutazione dei rischi e di impatto, con l'eventuale consultazione preventiva
- Misure di sicurezza adeguate a rischi
- Verifiche per il trasferimento dei dati extra UE
- Accordi e contratti
- Designazione delle persone autorizzate che svolgono funzioni e compiti connessi con il trattamento
- Formazione ed istruzioni
- Tenuta dei registri delle attività di trattamento
- Notificazione e comunicazione delle violazioni dei dati

E più in generale tutte le misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento devono essere riesaminate e

aggiornate periodicamente qualora necessario.

Inoltre almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto

Conclusione del trattamento

Reg.(UE)2016/679 considerando 39

- Per assicurare che i dati personali non siano conservati più a lungo del necessario, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica
- Alternativa alla cancellazione è l'Anonimizzazione. Infatti il GDPR non si applica al trattamento di tali informazioni anonime

Conclusione del trattamento

Per assicurare che i dati personali non siano conservati più a lungo del necessario, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica e quindi

Cancellare i dati al termine del periodo di conservazione

Oppure in Alternativa alla cancellazione dovrebbe ricorrere all'Anonimizzazione attraverso un processo tale da impedire o da non consentire più l'identificazione dell'interessato) Infatti il GDPR non si applica al trattamento di tali informazioni anonime

Garanzia e Dimostrazione di conformità

Reg.(UE)2016/679 art. 24 co. 

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per

1. garantire ed
2. essere in grado di dimostrare

che il trattamento è effettuato conformemente al regolamento.

- 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

Possibile dimostrazione di conformità

Reg.(UE)2016/679 art. 24 co. 

L'adesione a

- codice di condotta (articolo 40) o
- meccanismo di certificazione (articolo 42)

può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento