

Il nuovo pacchetto Privacy, confronto tra passato e futuro della normativa: GDPR e direttiva 2016/680

Avv. Gianbattista Causin

causin@forovenezia.it

Venezia – Dorsoduro 3480/a

Security Summit - Treviso 2017

Carta dei diritti fondamentali dell'UE

Articolo 8 -Protezione dei dati di carattere personale

1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano.
2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o ad un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica.
3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente

Principi applicabili al trattamento di dati personali

- a) liceità, correttezza e trasparenza;
- b) limitazione della finalità;
- c) minimizzazione dei dati;
- d) esattezza;
- e) limitazione della conservazione;
- f) integrità e riservatezza;

Il titolare del trattamento è competente per il rispetto di tali principi e in grado di provarlo

(«**responsabilizzazione**»)

Cambio di prospettiva

La **direttiva 95/46/CE** ha introdotto un **obbligo generale di notificare** alle autorità di controllo il trattamento dei dati personali. Mentre tale obbligo comporta oneri amministrativi e finanziari, non ha sempre contribuito a migliorare la protezione dei dati personali. È pertanto opportuno **abolire tali obblighi generali e indiscriminati di notifica e sostituirli con meccanismi e procedure efficaci** che si concentrino piuttosto su quei tipi di trattamenti che potenzialmente presentano un rischio elevato per i diritti e le libertà delle persone fisiche, per loro natura, ambito di applicazione, contesto e finalità. Tali tipi di trattamenti includono, in particolare, quelli che comportano l'utilizzo di nuove tecnologie o quelli che sono di nuovo tipo e in relazione ai quali il titolare del trattamento non ha ancora effettuato una valutazione d'impatto sulla protezione dei dati, o la valutazione d'impatto sulla protezione dei dati si riveli necessaria alla luce del tempo trascorso dal trattamento iniziale .

Principi applicabili al trattamento di dati personali

Il **bilanciamento** fra legittimo interesse del titolare o del terzo ed i diritti e le libertà dell'interessato

NON SPETTA all'Autorità ma **è compito dello stesso titolare valutare il bilanciamento**

Spetta al titolare anche valutare se ogni **ulteriore trattamento** è compatibile con la finalità del consenso già prestato (art. 6, 4° comma)

Nuovi istituti

- DPO
- DPIA – Valutazione di impatto sulla protezione dei dati
- Registri
- Portabilità

Nuove tutele

- Limitazione del trattamento
- Opposizione all'automatizzazione
- Sanzioni
- Direttiva 2016/680
- Consenso dei minori

Fondamenti di liceità del trattamento



- Per i dati "sensibili" il consenso **DEVE** essere "esplicito"; lo stesso dicasi per il consenso a 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); inoltre, 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 16 anni**; prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci

Fondamenti di liceità del trattamento



I **legittimi interessi di un titolare** del trattamento, compresi quelli di un titolare del trattamento a cui i dati personali possono essere comunicati, o di terzi possono costituire una base giuridica del trattamento, **a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato**, tenuto conto delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento.

Legittimi interessi di un titolare: quando esista una relazione pertinente e appropriata tra l'interessato e il titolare del trattamento, ad esempio **quando l'interessato è un cliente o è alle dipendenze del titolare del trattamento**.

Può essere considerato legittimo interesse trattare dati personali per finalità di **marketing diretto**.

Fondamenti di liceità del trattamento



Il consenso raccolto precedentemente al 25 maggio 2018 resta valido.

Il consenso è revocato con la stessa facilità con cui è accordato.

Per valutare se il consenso è stato liberamente rilasciato può essere utile **verificare se il consenso è necessario alla prestazione del servizio.**

INFORMATIVA



Il regolamento specifica molto più in dettaglio rispetto al Codice le caratteristiche dell'informativa:

forma **concisa, trasparente, intelligibile** per l'interessato e **facilmente accessibile**;

occorre utilizzare un linguaggio **chiaro e semplice** (soprattutto per i minori).

in linea di principio, per iscritto e preferibilmente in formato elettronico.

Sono anche previsti casi per i quali il titolare è esonerato dall'obbligo di fornire l'informativa.

INFORMATIVA



Nel caso di dati personali non raccolti direttamente presso l'interessato (*art. 14 del regolamento*), l'informativa deve essere fornita **entro un termine ragionevole che non può superare 1 mese** dalla raccolta,
oppure,
se servivano a contattare il cliente, **al momento del primo contatto con l'interessato.**

Se trasferiti a terzi, prima del trasferimento

Diritti degli interessati



- **Accesso**
- **Cancellazione/Oblio**
- **Limitazione del Trattamento**
- **Opposizione**
- **Portabilità**
- **Opposizione all'automatizzazione**

ACCESSO



Forma concisa, trasparente, **intelligibile** e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.

Al più tardi **entro un mese** dal ricevimento della richiesta stessa, e comunque **non oltre tre mesi totali**, tenuto conto della complessità e del numero delle richieste.

I motivi del ritardo, sempre entro un mese.

Gratuito. Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento può: a) addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta; oppure b) rifiutare di soddisfare la richiesta.

Codice 196/2003

Limitazioni all'accesso

Art. 8, 2. I diritti di cui all'articolo 7 non possono essere esercitati con richiesta al titolare o al responsabile o con ricorso ai sensi dell'articolo 145, se i trattamenti di dati personali sono effettuati:

- a) in base alle disposizioni del decreto legge 3 maggio 1991, n. 143, in materia di riciclaggio;
- b) in base alle disposizioni del decreto legge 31 dicembre 1991, n. 419 in materia di sostegno alle vittime di richieste estorsive;
- c) da Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione;
- d) da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità;
- e) ai sensi dell'articolo 24, comma 1, lettera f), limitatamente al periodo durante il quale potrebbe derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive o per l'esercizio del diritto in sede giudiziaria;
- f) da fornitori di servizi di comunicazione elettronica accessibili al pubblico relativamente a comunicazioni telefoniche in entrata,
- g) per ragioni di giustizia,

Cancellazione/Oblio



Interesse pubblico alla conoscenza di un fatto che con il passare del tempo si affievolisce, mentre aumenta il diritto dell'interessato alla cancellazione del dato.

Cancellazione/Oblio

Sentenza CEDU 9 marzo 2017, n. 398/15



Spetta agli Stati membri determinare se le persone fisiche di cui all'articolo 2, paragrafo 1, lettere d) e j), della direttiva 68/151 (2003/58) possano chiedere all'autorità incaricata della tenuta, rispettivamente, del registro centrale, del registro di commercio o del registro delle imprese di verificare, **in base ad una valutazione da compiersi caso per caso**, se sia eccezionalmente giustificato, per ragioni preminenti e legittime connesse alla loro situazione particolare, **decorso un periodo di tempo sufficientemente lungo dopo lo scioglimento della società interessata, limitare l'accesso ai dati personali che le riguardano**, iscritti in detto registro, ai terzi che dimostrino un interesse specifico alla loro consultazione

Cancellazione/Obligo

NON APPLICABILE



- a) per l'esercizio del diritto alla **libertà di espressione e di informazione**;
- b) per l'**adempimento di un obbligo legale** che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
- c) per **motivi di interesse pubblico nel settore della sanità pubblica** in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;
- d) a **fini di archiviazione nel pubblico interesse**, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o
- e) per l'accertamento, l'esercizio o la difesa di un **diritto in sede giudiziaria**

Cancellazione/Oblio/Rettifica

doc. web n. 5690019 – Newsletter 421/2016



Il diritto della persona di ottenere l'aggiornamento delle informazioni che lo riguardano deve essere comunque garantito qualora eventi successivi abbiano modificato quanto riportato, incidendo in modo significativo sul suo profilo e sulla sua immagine.

L'aggiornamento, inoltre, per salvaguardare l'attuale identità sociale della persona deve essere effettivo e non limitato ad una postilla poco visibile.

Limitazione



Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la limitazione è vietato a meno che ricorrano determinate circostanze .

E' necessario che il titolare predisponga un "archivio" o una "opzione" specifica per i dati trattati che non possa ancora cancellare.

Opposizione all'automatizzazione



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.

Almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione, quando:

- a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
- b) ;
- c) si basi sul consenso esplicito dell'interessato;

PORTABILITÀ

Linee-guida sul diritto alla “portabilità dei dati”



Il diritto alla portabilità dei dati permette agli interessati di ricevere i dati personali da loro forniti al titolare, in un **formato** strutturato, **di uso comune** e leggibile meccanicamente, e di trasmetterli a un diverso titolare. L'obiettivo ultimo è accrescere il controllo degli interessati sui propri dati personali .

Sarebbe buona prassi che i titolari di trattamento iniziassero a mettere a punto gli strumenti che faciliteranno l'esercizio del diritto alla portabilità – per esempio, strumenti per il download dei dati e API (interfacce di programmazione di applicazioni).

in un formato strutturato, di uso comune e leggibile meccanicamente e li si dovrebbe invitare a **garantire l'interoperabilità dei formati** con cui i dati vengono messi a disposizione in ottemperanza a una richiesta di portabilità .

Nel parere **si raccomanda al mondo imprenditoriale e alle associazioni di settore di collaborare in vista della definizione di un insieme condiviso di standard e formati interoperabili che soddisfino i requisiti del diritto alla portabilità dei dati**

Titolare, responsabile, incaricato del trattamento



Le precedenti versioni italiane del Regolamento riportavano i termini *"responsabile del trattamento"* (data controller) e *"incaricato del trattamento"* (data processor). Tuttavia, trattandosi, di fatto, di figure identiche quanto a caratteristiche soggettive a quelle che nel Codice privacy italiano sono indicate rispettivamente come "titolare" e "responsabile", l'Autorità italiana ha chiesto ed ottenuto che i nuovi testi mantenessero tali diciture.

Il regolamento definisce **caratteristiche soggettive e responsabilità di titolare e responsabile del trattamento** negli stessi termini di cui alla direttiva 95/46/CE (e, quindi, al Codice italiano). Pur non prevedendo espressamente la **figura dell' "incaricato" del trattamento** (ex art. 30 Codice), il regolamento **non ne esclude** la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile" (*si veda, in particolare, art. 4, n. 10, del regolamento*

Approccio basato sul rischio del trattamento e misure di **accountability** di titolari e responsabili



- Valutazione di Impatto
- Registro dei Trattamenti
- Misure di Sicurezza
- Violazioni dei Dati Personali
- Nomina di un Rdp/Dpo

Registri delle attività di trattamento

Devono essere predisposti dal titolare e/o dal responsabile (incaricato).

- Imprese con più di **250 dipendenti**,
- in caso di rischi per i diritti e le libertà dell'interessato,
- il trattamento non sia occasionale o includa il trattamento di dati sensibili o giudiziari (arrrt. 9 e 10).

Nomina di un Rdp/Dpo

Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualevolta:

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

Nomina di un Rdp/Dpo

- Autorità pubblica o organismo pubblico
- Attività principali
- Larga scala
- Monitoraggio regolare e sistematico di interessati

Esempi

- Ricerche di Mercato
- Reindirizzamento di Messaggi Di Posta
- Tracciamento di Ubicazione
- Utilizzo di Telecamere a Circuito Chiuso
- Gestione di Dispositivi per la Domotica

Funzioni del Rdp/Dpo

- informare e fornire consulenza
- sorvegliare l'osservanza del presente regolamento
- fornire, se richiesto, un parere
- cooperare con l'autorità di controllo;
- fungere da punto di contatto per l'autorità di controllo

Articolo 35

Valutazione d'impatto sulla protezione dei dati

Quando un tipo di trattamento, allorché prevede **in particolare l'uso di nuove tecnologie**, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può **presentare** (NB “**is likely to result**”) **un rischio elevato per i diritti e le libertà delle persone fisiche**, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.

Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi

DPIA

A cosa serve?

L'esito della valutazione dovrebbe essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta il presente regolamento.

Laddove la valutazione d'impatto sulla protezione dei dati indichi che i trattamenti presentano un rischio elevato che il titolare del trattamento non può attenuare mediante misure opportune in termini di tecnologia disponibile e costi di attuazione, prima del trattamento si dovrebbe consultare l'autorità di controllo.

Premessa (84)

Articolo 35

Valutazione d'impatto sulla protezione dei dati

La valutazione d'impatto sulla protezione dei dati è richiesta in particolare nei casi seguenti:

- a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un **trattamento automatizzato, compresa la profilazione**, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- b) il trattamento, **su larga scala**, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o
- c) **la sorveglianza sistematica** su larga scala di una zona accessibile al pubblico

Articolo 35

Valutazione d'impatto sulla protezione dei dati

La valutazione contiene almeno:

- a) una descrizione sistematica dei trattamenti e delle finalità del trattamento, nonché l'interesse legittimo perseguito dal titolare del trattamento;
- b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- c) una valutazione dei rischi;
- d) le misure previste per affrontare i rischi,

DPIA

Coinvolgimento degli interessati

- Il titolare deve “cercare il punto di vista degli interessati o dei loro rappresentanti” (articolo 35 (9)), “se del caso”.

Il WP29 ritiene che:

- tali opinioni potrebbero essere ricercate attraverso una varietà di mezzi, a seconda del contesto (ad esempio, uno studio interno o esterno legato alla finalità e modalità dell'operazione di elaborazione, una domanda formale ai rappresentanti del personale, alle associazioni di categoria o ai sindacati o un sondaggio inviato ai futuri clienti del titolare del trattamento);
- se la decisione finale del titolare del trattamento differisce dal punto di vista degli interessati, i motivi per andare avanti o meno devono essere documentati;
- il titolare deve anche documentare le ragioni per non indagare il punto di vista delle persone interessate, se si decide che questo non è appropriato.

DPIA

Rischi

- distruzione accidentale o illegale,
- la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali

Quando c'è il rischio di cagionare in particolare un danno fisico, materiale o immateriale.

Premessa (83)

DPIA

Criteri

La valutazione o l'assegnazione di un punteggio

Decisioni automatiche con effetti giuridici o similmente significativi

Controllo sistematico

Dati Sensibili

I dati elaborati su larga scala

Set di dati che sono stati abbinati o combinati

I dati relativi interessati vulnerabili

L'uso innovativo o l'applicazione di soluzioni tecnologiche o organizzative

Il trasferimento dei dati attraverso i confini al di fuori dell'Unione europea

Quando l'elaborazione in sé "impedisce agli interessati di esercitare un diritto o utilizzare un servizio o un contratto"

Three cartoon monkeys are visible in the background, appearing to be part of a presentation or video. They are positioned behind the text, with one on the left, one in the center, and one on the right. They have large heads, expressive faces, and are wearing small hats or headbands.

DPIA

Obbligo per il titolare

Il soggetto a cui compete la redazione e l'aggiornamento di una **DPIA** è il Titolare del trattamento, eventualmente supportato ove previsto dal Data Protection Officer

DPIA

Forma e struttura libera

il **WP29** lascia **libertà di scelta per la forma e la struttura** da utilizzare, purché contenga gli elementi previsti dal GDPR ed esplicitati all'interno dell'Annex 2 delle Linee Guida

Articolo 35

Valutazione d'impatto sulla protezione dei dati

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.

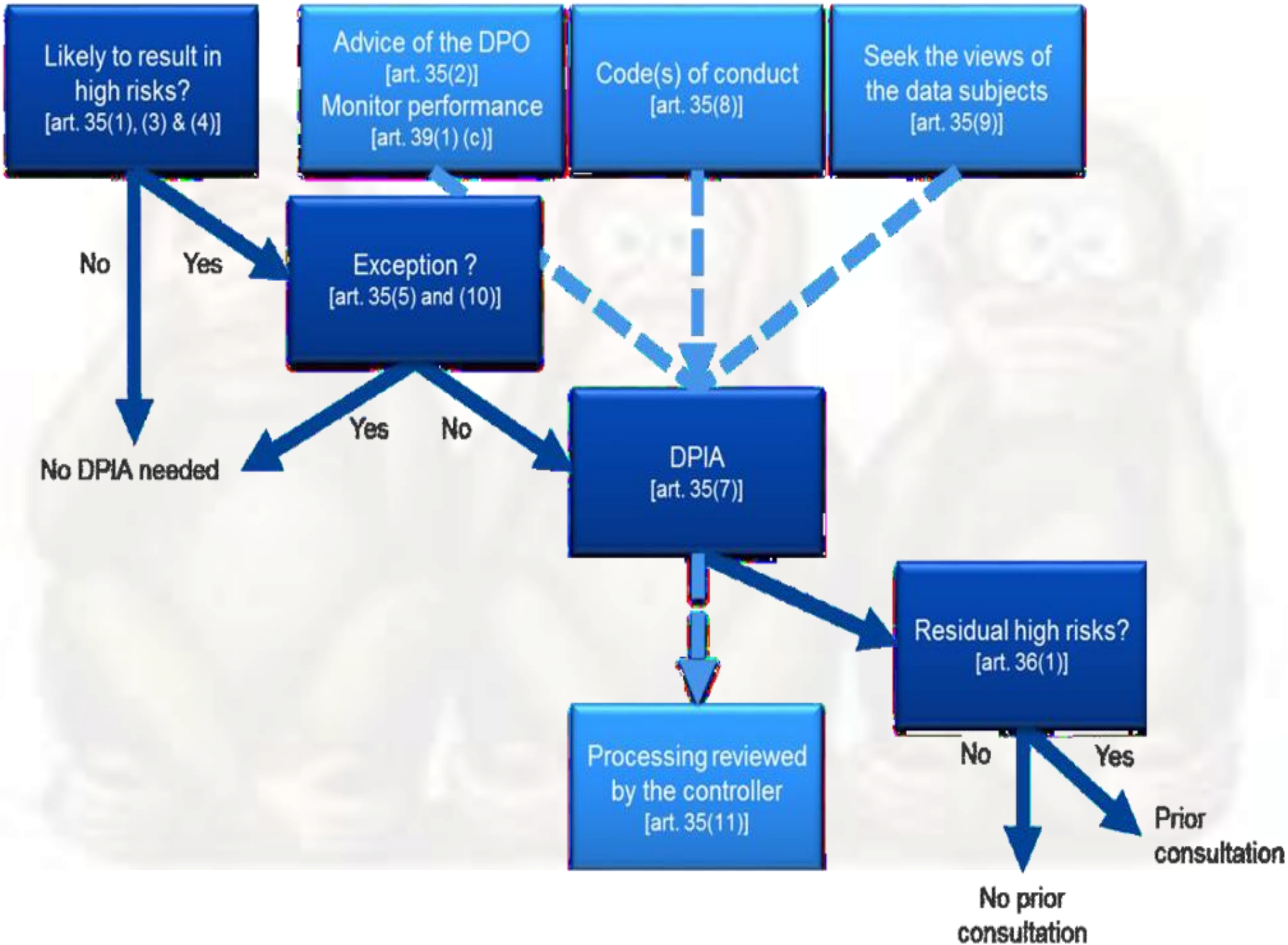
Entro 3 anni (linee guida WP29)

Articolo 35

Valutazione d'impatto sulla protezione dei dati

L'autorità di controllo redige e rende pubblico un **elenco delle tipologie di trattamenti soggetti** al requisito di una valutazione d'impatto.

L'autorità di controllo può inoltre redigere e rendere pubblico un **elenco** delle tipologie di trattamenti **per le quali non è richiesta** una valutazione d'impatto



Coordinamento tra Regolamento e Codice della Privacy

L'ordinamento comunitario e l'ordinamento statale sono "distinti e al tempo stesso coordinati" e le norme del primo vengono, in forza dell'art. 11 Cost., a ricevere diretta applicazione in quest'ultimo, pur rimanendo estranee al sistema delle fonti statali; da ciò deriva non la caducazione della norma interna incompatibile bensì la non applicazione di quest'ultima da parte del giudice nazionale al caso di specie oggetto della sua cognizione

Decreto legislativo 08.06.2001, n. 231

Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300 per gli illeciti amministrativi dipendenti da reato

Decreto legislativo 08.06.2001, n. 231

1. L'ente è responsabile per i reati commessi nel suo interesse o a suo vantaggio:
 - a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso
 - b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a).
2. L'ente non risponde se le persone indicate nel comma 1 hanno agito nell'interesse esclusivo proprio o di terzi.

Decreto legislativo 14 marzo 2013, n. 33

Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni

Art. 1. Principio generale di trasparenza

1. La trasparenza è intesa come **accessibilità totale dei dati e documenti detenuti dalle pubbliche amministrazioni**, allo scopo di tutelare i diritti dei cittadini, promuovere la partecipazione degli interessati all'attività amministrativa e favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche.
2. La trasparenza, nel rispetto delle disposizioni in materia di segreto di Stato, di segreto d'ufficio, di segreto statistico e di protezione dei dati personali, concorre ad attuare il principio democratico e i principi costituzionali di eguaglianza, di imparzialità, buon andamento, responsabilità, efficacia ed efficienza nell'utilizzo di risorse pubbliche, integrità e lealtà nel servizio alla nazione. **Essa è condizione di garanzia delle libertà individuali e collettive, nonché dei diritti civili, politici e sociali**, integra il diritto ad una buona amministrazione e concorre alla realizzazione di una amministrazione aperta, al servizio del cittadino

Statuto dei lavoratori

art. 4

1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale .

In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione dell'Ispettorato nazionale del

I provvedimenti di cui al terzo periodo sono definitivi.

2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.

3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196.

T.U.B.

Il cliente, colui che gli succede a qualunque titolo e colui che subentra nell'amministrazione dei suoi beni hanno diritto di ottenere, a proprie spese, entro un congruo termine e comunque non oltre novanta giorni, copia della documentazione inerente a singole operazioni poste in essere negli ultimi dieci anni.

Al cliente possono essere addebitati solo i costi di produzione di tale documentazione.

Direttiva 2016/680

Protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati.

Direttiva 2016/680

gli Stati membri:

- a) tutelano i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali; e
- b) garantiscono che lo scambio dei dati personali da parte delle autorità competenti all'interno dell'Unione non sia limitato né vietato per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali

Direttiva 2016/680

principio di attribuzione

La presente direttiva non si applica ai trattamenti di dati personali:

- a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione (questioni connesse alla sicurezza nazionale e il trattamento dei dati personali effettuato dagli Stati membri nell'esercizio di attività rientranti nell'ambito di applicazione del titolo V, capo 2, del trattato sull'Unione europea (TUE) – premessa 14;
- b) effettuati da istituzioni, organi, uffici e agenzie dell'Unione – Regolamento 45/2001

Direttiva 2016/680

Il regolamento (UE) 2016/679 si applica pertanto nei casi in cui un organismo o un'entità raccolgano dati personali per finalità diverse e procedano a un loro ulteriore trattamento per adempiere un obbligo legale cui sono soggetti.

Ad esempio, a fini di indagine, accertamento o perseguimento di reati, gli istituti finanziari conservano determinati dati personali da essi trattati, e li trasmettono solo alle autorità nazionali competenti in casi specifici e conformemente al diritto dello Stato membro. Un organismo o un'entità che trattano dati personali per conto di tali autorità entro l'ambito di applicazione della presente direttiva dovrebbero essere vincolati da un contratto o altro atto giuridico e dalle disposizioni applicabili ai responsabili del trattamento a norma della presente direttiva;

Direttiva 2016/680

L'applicazione del regolamento (UE) 2016/679 rimane invece impregiudicata per le attività di trattamento svolte dal responsabile del trattamento di dati personali al di fuori dell'ambito di applicazione della presente direttiva.

Direttiva 2016/680

Gli Stati membri possono conferire alle autorità competenti altri compiti che non siano necessariamente svolti a fini di prevenzione, indagine, accertamento o perseguimento di reati, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, cosicché il trattamento di dati personali per tali altre finalità, nella misura in cui ricada nell'ambito di applicazione del diritto dell'Unione, rientra nell'ambito di applicazione del regolamento (UE) 2016/679

Direttiva 2016/680

Diritto all'accesso

Gli Stati membri dispongono che l'interessato abbia il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano.

Gli Stati membri possono adottare misure legislative volte a **limitare**, in tutto o in parte, il diritto di accesso dell'interessato nella misura e per il tempo in cui tale limitazione totale o parziale costituisca una misura necessaria e proporzionata:

- a) non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari;
- b) non compromettere la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali;
- c) proteggere la sicurezza pubblica;
- d) proteggere la sicurezza nazionale;
- e) proteggere i diritti e le libertà altrui

Direttiva 2016/680

Obbligo informativo

Gli Stati membri dispongono che il titolare del trattamento informi l'interessato, senza ingiustificato ritardo e per iscritto, di ogni rifiuto o limitazione dell'accesso e dei motivi del rifiuto o della limitazione.

Detta comunicazione può essere omessa qualora il suo rilascio rischi di compromettere una delle finalità di cui al paragrafo 1. Gli Stati membri dispongono che il titolare del trattamento informi l'interessato della possibilità di proporre reclamo dinanzi a un'autorità di controllo o di proporre ricorso giurisdizionale. 4.

Gli Stati membri dispongono che il titolare del trattamento documenti i motivi di fatto o di diritto su cui si basa la decisione. Tali informazioni sono rese disponibili alle autorità di controllo.

Direttiva 2016/680

Consenso

il consenso dell'interessato, quale definito nel regolamento (UE) 2016/679, non dovrebbe costituire la base giuridica per il trattamento di dati personali da parte delle autorità competenti.

Qualora sia tenuto ad adempiere un obbligo legale, l'interessato non è in grado di operare una scelta autenticamente libera, pertanto la sua reazione non potrebbe essere considerata una manifestazione di volontà libera.

Ciò non dovrebbe impedire agli Stati membri di prevedere per legge che l'interessato possa acconsentire al trattamento dei propri dati personali ai fini della presente direttiva, ad esempio per test del DNA nell'ambito di indagini penali o per il monitoraggio della sua ubicazione mediante dispositivo elettronico per l'esecuzione di sanzioni penali

Direttiva 2016/680

- diritto di rettifica o cancellazione;
- privacy by design e privacy by default;
- DPIA;
- contitolari del trattamento;
- responsabile del trattamento;
- Registri;
- comunicazione delle violazioni;
- DPO

Direttiva 2016/680

principio di sussidiarietà

Poiché gli obiettivi della presente direttiva non possono essere conseguiti in misura sufficiente dagli Stati membri ma piuttosto possono essere conseguiti meglio a livello di Unione, quest'ultima può intervenire.

Direttiva 2016/680

Tutele

Nei casi di cui all'articolo 13, paragrafo 3, all'articolo 15, paragrafo 3, e all'articolo 16, paragrafo 4, gli Stati membri adottano misure che dispongano che i diritti dell'interessato possano essere esercitati anche tramite l'autorità di controllo competente.

Qualora sia esercitato il diritto di cui al paragrafo 1, l'autorità di controllo informa l'interessato, perlomeno, di aver eseguito tutte le verifiche necessarie o un riesame.

Ciascun interessato ha il diritto di proporre un ricorso giurisdizionale effettivo qualora l'autorità di controllo non tratti un reclamo o non lo informi entro tre mesi dello stato o dell'esito del reclamo.

Direttiva 2016/680

Sanzioni

Le sanzioni previste devono essere effettive, proporzionate e dissuasive.



Direttiva 2016/680

Entrata in vigore

Gli Stati membri adottano e pubblicano, entro il **6 maggio 2018**, le disposizioni legislative, regolamentari e amministrative necessarie per conformarsi alla presente direttiva.

In **deroga** al paragrafo 1, uno Stato membro può disporre che, in via eccezionale, qualora ciò comporti sforzi sproporzionati, i sistemi di trattamento automatizzato istituiti anteriormente al 6 maggio 2016 siano resi conformi all'articolo 25, paragrafo 1, entro il 6 maggio **2023**.

Ulteriore deroga il termine specificato può arrivare fino al 6 maggio **2026**