European Commission

CONSULTING

IL REGOLAMENTO UE 2016 / 679: COME CAMBIERÀ LA PRIVACY IN AZIENDA DAL 2018?

Moduli

1. Il nuovo Regolamento, principi, definizioni e nuovi attori
2. Diritti degli interessati, informativa e consenso, cosa cambia?
3. Le figure previste, titolare, responsabile, responsabile della protezione dati e incaricati, nuovi obblighi e nuove responsabilità
4. I nuovi adempimenti del titolare verso l'autorità di controllo
5. Trasferimento verso paesi terzi ed organizzazioni internazionali (cenni)
6. Sistema sanzionatorio e diritto al risarcimento, responsabilità del titolare.

1 Il nuovo Regolamento, definizioni, principi e nuovi attori

Mappa dell'argomento:

DEFINIZIONI

- Nuove definizioni, concetti, figure…
- Ambito di applicazione (art. 3 GDPR)

PRINCIPI (RESPONSABILIZZAZIONE) E TRATTAMENTI DI CATEGORIE PARTICOLARI DI DATI PERSONALI

- Principi (art. 5 GDPR)
- Liceità (art. 6 GDPR)
- Trattamento di categorie particolari di dati personali (art. 9 GDPR)

Il nuovo Regolamento, definizioni, principi e nuovi attori

Nuove definizioni, concetti, figure…

GDPR (RGPD)

General Data Protection Regulation, ovvero **Regolamento Generale sulla Protezione dei Dati** è l'acronimo inglese che indica il Regolamento Europeo sulla Protezione dei Dati 2016 / 679. Sostituirà la normativa applicata nei diversi stati e la unificherà nei 27 stati membri, avrà effetti dal 25 maggio 2018. In italiano l'acronimo diventa **RGPD** (**R**egolamento **G**enerale sulla **P**rotezione dei **D**ati). Il Regolamento stabilisce norme relative alla protezione delle **persone fisiche** con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati (art.1 GDPR).

ACCOUNTABILITY

Ovvero obbligo di documentazione e analisi dei rischi (*risk based approach*).

DPIA (Data Protection Impact Assessment)

Valutazione degli impatti privacy del processo aziendale e degli strumenti informatici a supporto.

DATA BREACH

Ovvero obbligo di notifica all'autorità di controllo di denunciare una violazione dei dati personali (art. 33 GDPR).

WP 29

Working Party 29 (l'organismo indipendente che raggruppa i Garanti Privacy europei)

DIRITTO ALL'OBLIO

L'interessato dovrebbe avere il diritto di chiedere che siano cancellati e non più sottoposti a trattamento i propri dati personali che non siano più necessari per le finalità per le quali sono stati raccolti o altrimenti trattati, quando abbia ritirato il proprio consenso o si sia opposto al trattamento dei dati personali che lo riguardano o quando il trattamento dei suoi dati personali non sia altrimenti conforme al presente regolamento (Art. 17 RGDP).

* Interessato = **Persona fisica** a cui si riferisca il dato personale e che la renda identificabile (compreso identificativo *on line*).

PRIVACY BY DESIGN

Esplicitazione del principio dell'incorporazione delle pratiche di protezione dei dati personali fino dalla progettazione del processo aziendale.

PROFILAZIONE

Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati per valutare determinati aspetti dell'interessato, in particolare per analizzare o prevedere il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti.

PSEUDONOMIZZAZIONE

Il trattamento di dati personali organizzato perché non sia possibile attribuire il dato ad 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 volte ad garantire tale misura.

TITOLARE

Persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità ed i mezzi del trattamento di dati personali.

RAPPRESENTANTE

In pratica è la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile per iscritto ai sensi dell'art. 27 RGDP, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento.

RESPONSABILE

Soggetto a cui ricorre il titolare qualora deleghi a terzi un trattamento per proprio conto.

RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD - DPO)

Figura obbligatoriamente prevista in determinate fattispecie (Art. 37 RGDP), viene comunemente chiamata *Data Protection Officer* (DPO).

DESTINATARIO

Il destinatario è una nuova figura non presente nel 196/2003. È la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che riceve comunicazione dei dati personali, che si tratti o meno di terzi.

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

RESPONSABILIZZAZIONE
Obbligo del titolare di comprovare i principi di correttezza, liceità e trasparenza del trattamento dei dati.

DIRITTO ALLA PORTABILITÀ DEI DATI
È tale il diritto che consiste nella possibilità di richiedere al titolare una copia dei dati oggetto del trattamento. Oltre al diritto di ricevere copia dei dati, l'interessato ha diritto di trasmetterli ad altro titolare del trattamento, senza che il primo titolare possa porre alcun impedimento al trasferimento.
L'interessato può, infine, richiedere, anche, la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, purché ciò sia tecnicamente fattibile.

PROCESSO DECISIONALE AUTOMATIZZATO
La definizione scientifica di sistema di supporto automatizzato alle decisioni dovrebbe essere un sistema che aiuta l'utente a prendere le decisioni ma senza sostituirsi ad esso. Ed è proprio conformemente a questa definizione tecnica che il Regolamento prevede che un determinato trattamento automatizzato (come la profilazione) NON sia effettuata univocamente da algoritmi senza l'intervento dell'interessato, magari producendo addirittura effetti giuridici per quest'ultimo.

LIMITAZIONE DEL TRATTAMENTO

Limitare un trattamento significa interrompere l'uso del dato per un determinato periodo, magari a fronte di una verifica di liceità o limitarne l'uso a particolare trattamento escludendone altri (quando possibile per l'esecuzione della prestazione fra le parti).

CODICI DI CONDOTTA

Sono dei modelli che possono essere elaborati da associazioni di categoria, piuttosto che da altri organismi rappresentanti categorie di titolari, destinati a contribuire alla corretta applicazione del presente regolamento, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese.

MECCANISMO DI CERTIFICAZIONE

Meccanismo che accerti la conformità al presente Regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento.

COMITATO

Il comitato europeo per la protezione dei dati («comitato» o CEPD) è istituito quale organismo dell'Unione ed è dotato di personalità giuridica, garantisce l'applicazione coerente del presente regolamento. In particolare pubblica linee guida, incoraggia l'uso di codici di condotta e di meccanismi di certificazione, accreditandone gli organismi certificatori.

RESILIENZA DEI DATI

La resilienza dati è la capacità da parte dei dati di essere disponibili per gli utenti o le applicazioni anche dopo eventi dannosi.

DATO PERSONALE

Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

CATEGORIE PARTICOLARI DI DATI PERSONALI (EX DATI SENSIBILI)

Nel Regolamento non si usa più la definizione di dati sensibili come categoria di dati personali, ma si usa la definizione di "categorie particolari di dati personali" che nella fattispecie sono quelli atti ad indicare:

_ Origine razziale o etnica;
_ Le opinioni politiche;
_ Le convinzioni religiose o filosofiche;
_ L'appartenenza sindacale;
_ Dati genetici;
_ Dati biometrici intesi a identificare in modo univoco una persona fisica;
_ Dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Ambito di applicazione (art. 3 GDPR)

Ambito di applicazione materiale

Il regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un **archivio*** o destinati a figurarvi.

***Archivio** = Secondo il GDPR la definizione di archivio è qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico; La definizione analoga nel D.lgs. 196/2003 era quella di banca dati.

Ambito di applicazione territoriale

Il regolamento viene applicato al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.

→ Quindi se il trattamento è effettuato da un qualunque soggetto dell'Unione (anche se non fisicamente effettuato in Unione) è soggetto al regolamento o se è rivolto verso soggetti interessati nell'Unione o anche se il trattamento è rivolto ad uno stato membro in virtù del diritto internazionale.

Principi (art. 5 GDPR)

In sintesi i principi applicabili ad un trattamento di dati personali elencati al Comma 1 dell'art.5 GDPR sono i seguenti:

a) Liceità, correttezza e trasparenza;
b) Limitazione della finalità;
c) Minimizzazione dei dati;
d) Esattezza (criterio dei dati esatti e aggiornati);
e) Limitazione della conservazione;
f) Integrità e riservatezza.

Al Comma 2 si riporta:
Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).

→ Il Comma 1 di questo articolo riprende pedissequamente l'art. 11 del D.lgs. 196/2003 titolato "Modalità del trattamento e requisiti dei dati" andando semplicemente ad approfondirne la ratio con delle spiegazioni maggiormente esaustive, ma riprendendo tutti i concetti del lecito e sicuro trattamento (liceità, correttezza e trasparenza).

Invece il Comma 2 sostituisce quello del 196 con un concetto che apre un mondo nuovo, ovvero che il **titolare è competente** e deve essere in grado di comprovare il rispetto di questi principi e questa attitudine viene definita Responsabilizzazione.

Liceità (art. 6 GDPR)

Il regolamento conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica; **i fondamenti di liceità del trattamento sono indicati all'art. 6 del regolamento e coincidono, in linea di massima, con quelli previsti attualmente dal Codice** (consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri**, interesse legittimo prevalente del titolare rispetto a quello dell'interessato**).

L'ultimo punto è quello maggiormente degno di riflessione, infatti il concetto di **responsabilizzazione**, introdotto nel precedente articolo, vede il titolare come il soggetto investito nella determinazione del cosiddetto principio di "bilanciamento degli interessi", non spetta perciò all'Autorità determinare quale sia il diritto prevalente fra il proprio e quello dell'interessato. Naturalmente il titolare chiamato in causa dovrà giustificare i motivi delle proprie decisioni.

Il Garante porta come esempio di trattamento effettuato in mancanza di consenso quello effettuato a fini di videosorveglianza quando sussistano motivi legati alla tutela del patrimonio o da esigenze di sicurezza anche personale.

Ad estensione di questo concetto nel comma 4 dell'art.6 GDPR si indica che spetta al titolare valutare se un trattamento di dati raccolti per finalità diverse sia legittimo incrociando alcune valutazioni quali il nesso fra le finalità originariamente indicate e le ulteriori, il contesto della raccolta, della natura dei dati e delle garanzie (anche tecniche) del trattamento.

Trattamento di categorie particolari di dati personali (art. 9 GDPR)

L'art. 9 al comma 1 **vieta** il trattamento di Categorie particolari di dati personali, (prima cosa che salta all'occhio è l'abbandono della definizione di dati sensibili) salvo eccezioni, vediamo le maggiormente significative indicate al comma 2:

- L'interessato ha prestato il proprio consenso esplicito al trattamento;
- Trattamento finalizzato all'adempimento di obblighi come in materia di lavoro e igiene e sicurezza nei luoghi di lavoro;
- Trattamento necessario per tutelare un interesse vitale nel caso di incapacità nell'esprimere il consenso (esempio del paziente al pronto soccorso in gravi condizioni);
- Il trattamento è effettuato con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro per finalità politiche, filosofiche, religiose o sindacali, solo se il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione nell'impegno di non comunicare a terzi o diffondere i dati;
- Il trattamento riguardi dati resi manifestamente pubblici dall'interessato (apparente contraddizione ma motivata dalla logica);
- Trattamento per finalità difensive in sede giudiziaria;
- Trattamento necessario per medicina preventiva, del lavoro, delle capacità del lavoratore, ecc;
- Altri casi riguardanti l'interesse pubblico.

Al Comma 3 si specifica che quelle categorie di dati possono essere comunque trattate da soggetti obbligati al segreto professionale, al 4 si lasciano aperte ipotesi di integrazione dei singoli stati membri.

2 Diritti degli interessati, informativa e consenso, cosa cambia?

Mappa dell'argomento:

TRASPARENZA E MODALITÀ CON CUI DEVE ESSERE RESA L'INFORMATIVA

- Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti, art.12 GDPR

INFORMAZIONE E ACCESSO AI DATI PERSONALI

- Informativa dati raccolti presso l'interessato art.13 GDPR
- Informativa dati non ottenuti presso l'interessato art.14 GDPR
- Casi di esonero artt.13 e 14 GDPR

CONSENSO art.7 GDPR

Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti, art.12 GDPR

Il titolare adotta **misure appropriate** per fornire all'interessato l'**informativa** (artt. 13 e 14 GDPR) in forma:

_ concisa;

_ trasparente;

_ intelligibile e facilmente accessibile;

_ Adottando un linguaggio semplice e chiaro (in particolare per i minori).

Modalità con cui si può rendere l'informativa:

_ per iscritto;

_ con mezzi elettronici;

_le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato*.

*Il punto non è chiarissimo… sicuramente è un punto fermo che una informativa scritta (riportata su supporto cartaceo/digitale e inviata/consegnata al destinatario con evidenza della ricezione da parte del medesimo) costituisce prova obiettiva dell'assolvimento dell'obbligo da parte del titolare.

Riscontro all'interessato esercizio dei diritti

Nel caso l'interessato manifestasse la richiesta di avere informazioni sul trattamento o altro, il titolare deve darne riscontro salvo che riesca a dimostrare di non essere in grado di identificare l'interessato richiedente.

I tempi di riscontro (Commi 3 e 4) dicono entro un mese dalla richiesta, prorogabile a 2 mesi in particolari casi, ma subordinato alla comunicazione del ritardo all'interessato comunque entro il mese dalla richiesta.

La soddisfazione della richiesta deve avere carattere gratuito, a meno che (dietro richieste frequenti ed "eccessive") si possano aprire le seguenti modalità / eccezioni:

- Addebitare spese amministrative;
- Rifiutare motivando l'eccessività delle richieste.

Informativa dati raccolti presso l'interessato art.13 GDPR

In prima battuta si nota immediatamente che, a differenza del D.lgs. 196/2003 si distinguono i casi fra informativa per dati raccolti presso l'interessato e non (ex comma 4 art. 13 D.lgs. 196/2003).

Gli elementi da indicare nella Informativa art. 13 GDPR sono:
_ Identità e dati di contatto del titolare e dell'eventuale rappresentante designato nel territorio dello Stato;
_ I dati di contatto del responsabile della protezione dei dati. Rispetto al D.lgs. 196/2003 non si parla più di "responsabile del trattamento" ma di "responsabile della protezione dei dati" questa figura è disciplinata alla sezione 4 dall'art. 37 GDPR nella quale sono specificati i casi specifici in cui debba essere sistematicamente nominata.
_ Le finalità del trattamento così come richiesto nel D.lgs. 196/2003 ma dovrà essere indicata anche la base giuridica del trattamento;
_ Richiamo al principio di Responsabilizzazione art. 6 lettera f) dando comunque obbligo di indicare i legittimi interessi perseguiti dal titolare;
_ Non si parla più di indicare l'eventuale ambito di comunicazione ma di indicare le categorie di destinatari;
_ Si chiede, ove possibile, di indicare il / i paesi terzi cui potranno essere inviati i dati, questione specificatamente affrontata per quanto riguarda le garanzie nell'art. 46,48, 49 2 Comma.

---> Nel momento fisico in cui i dati passano dall'interessato al titolare per garantire adeguata correttezza e trasparenza dovranno essere altresì indicati:
_ a) dovrà essere indicato (prima non era necessario) il periodo di conservazione oppure i criteri per determinare tale periodo;

_ b) Deve essere indicato il diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi (c.d. Diritto all'oblio art. 17) o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, (quello che prima era ottemperato con l'indicazione dell'art. 7 D.lgs. 196), viene aggiunta la specifica del diritto alla portabilità dei dati (da Senato.it: "l'introduzione del diritto alla portabilità dei dati, vale a dire il diritto di trasferire i propri dati tra diversi sistemi elettronici senza che il responsabile del trattamento possa impedirlo", oppure da EUR LEX: "la libertà di trasferire i propri dati personali da un prestatore di servizi a un altro, senza impedimenti") da questo si evince anche quanto impatterà la nuova disciplina anche nei rapporti tra l'Autorità della Protezione dei dati e la nostra vita quotidiana, comunque il "diritto alla portabilità dei dati" è disciplinato anche in maniera dettagliata dall'art. 20 del GDPR.

_ c) Nel caso in cui il trattamento sia basato sull'art. 6 comma 1 e art. 9 par. 2 lettera a) (liceità da consenso al trattamento) si dovrà comunque dare all'interessato la possibilità di revocare il consenso in qualsiasi momento senza che questo, comunque, comporti l'illiceità del trattamento per il periodo antecedente la richiesta;

_ d) Diritto di porre reclamo all'autorità di controllo;

_ e) Bisogna indicare chiaramente se la comunicazione dei dati sia un obbligo di legge, sia necessaria per adempiere ad un determinato contratto e, come era previsto precedentemente, le conseguenze nel rifiutarsi di conferire i dati;

_ f) Qualora vi sia un processo decisionale automatizzato art. 22 Regolamento (compresa la profilazione) le logiche adottate, importanza e conseguenze del trattamento.

Al punto 3 si dice che se si intendesse usare i dati per finalità diverse si dovrà procedere ad informare l'interessato PRIMA del trattamento seguendo l'iter appena descritto.

Riassunto delle "novità" da inserire in informativa:

_ Dati di contatto del responsabile per la protezione dei dati (RPD – DPO);
_ Base giuridica per le finalità di trattamento;
_ Qualora il trattamento sia impostato secondo l'art. 6 lettera f) indicare il legittimo interesse perseguito dal titolare;
_ Indicazione delle categorie di destinatari;
_ Periodo di conservazione dei dati (o criteri per la determinazione);
_ Diritti di cui attenzione al diritto all'oblio ed alla novità relativa alla portabilità del dato;
_ Nel caso di processo decisionale automatizzato dovranno essere indicate le logiche applicate e le relative conseguenze.

Informativa dati non ottenuti presso l'interessato art.14 GDPR

Se i dati non sono ottenuti direttamente dall'interessato il titolare deve ottemperare a tutti gli obblighi dell'art 13 fornendo le informazioni all'interessato entro 30 gg dalla raccolta, fatti salvi i casi in cui:
_ a) L'interessato dispone già delle informazioni (potrebbe essere il caso in cui nell'informativa data all'interessato stesso fosse già presente nella filiera di comunicazione dei dati);
_ b) Effettuare questa attività implichi un impiego sproporzionato di mezzi, in questo caso (si menzionano ricerche scientifiche, archiviazioni su elenchi pubblici, ecc) bisognerà adottare un regime di particolari garanzie per gli interessati stessi;
_ c) Ottenimento o comunicazione dei dati sono espressamente previsti dal diritto comunitario, oppure i dati siano destinati a rimanere riservati secondo un obbligo di segreto professionale disciplinato dal diritto dell'Unione.

Casi di esonero dell'informativa

1_ I punti visti nell'art. 13 relativamente alla informativa da rendere all'interessato **non** si applicano se e nella misura in cui l'interessato dispone già delle informazioni;

2_ Nel caso in cui i dati siano raccolti presso soggetti diversi dall'interessato nel caso in cui sia manifestamente impossibile renderla oppure se nel caso siano il trattamento dei dati sia coperto da segreto professionale (lettera d) punto 5 art. 15).

3_ Qualora l'esonero di fornire l'informativa sia una misura necessaria e proporzionata in una società democratica per salvaguardare unità nazionale, difesa, sicurezza pubblica, ecc… (art. 23 par.1).

Cosa si deve fare per le informative rese prima del 25 maggio 2018?

E' opportuno che i titolari di trattamento **verifichino la rispondenza delle informative** attualmente utilizzate a tutti i criteri sopra delineati, con particolare riguardo ai **contenuti obbligatori** e alle **modalità di redazione**, in modo da apportare le modifiche o le integrazioni eventualmente necessarie prima del 25 maggio 2018.

Consenso art.7 GDPR

Se il trattamento è basato sul consenso, la prima condizione per la sua validità è che il titolare sia in grado di dimostrarne il conferimento da parte dell'interessato.

Sarà perciò indispensabile una progettazione dei flussi organizzativi volti alla raccolta ed ai principi di conservazione e reperibilità.

Se il consenso è prestato per una pluralità di finalità i consensi dovranno essere specifici e chiaramente distinguibili per materia.

Ad esempio se la raccolta di una mail personale è finalizzata alla erogazione di un particolare servizio ma la si volesse usare anche per finalità commerciali (es. newsletter) i consensi dovranno essere specifici e distinguibili.

Il consenso può essere revocato in qualsiasi momento e la modalità deve risultare parimenti agibile al suo conferimento.

Nella valutazione se il consenso sia stato liberamente prestato, l'autorità tiene in massima considerazione la circostanza in cui in cui l'esecuzione di un contratto sia condizionata all'espressione di tale consenso non necessario alla esecuzione del contratto stesso.

Cosa vuole dire? Che se è stato raccolto un consenso relativo ad un trattamento di dati non strettamente connesso alla esecuzione di un determinato contratto si è orientati a valutare questa espressione non liberamente prestata…

Alcune domande / chiarimenti in merito al consenso…

Come deve essere reso per il trattamento di categorie particolari di dati (dati sensibili)?
Per i dati "sensibili" (si veda art. 9 regolamento) il consenso **DEVE** essere "esplicito"; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione – art. 22).

In che forma deve essere espresso?
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).

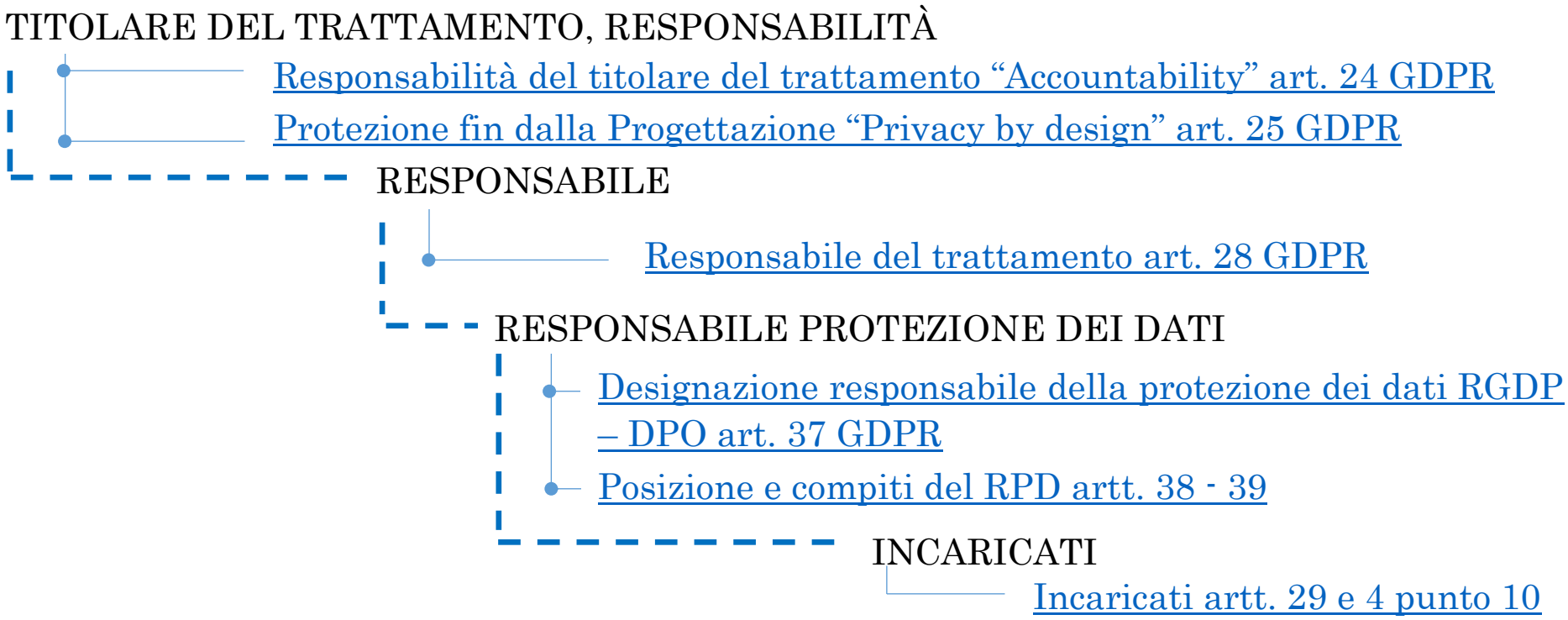
E per i minori?
Il **consenso dei minori** è valido **a partire dai 16 anni**; prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci.

Cosa si deve fare per i consensi resi prima del 25 maggio 2018?
Il consenso raccolto precedentemente al 25 maggio 2018 resta valido se ha tutte le caratteristiche sopra individuate. In caso contrario, è opportuno adoperarsi prima di tale data per raccogliere nuovamente il consenso degli interessati secondo quanto prescrive il regolamento.

Nei moduli, qualche accorgimento?
No a caselle pre-spuntate sui moduli (sia cartacei che informatici).

3 Le figure previste, titolare, responsabile, responsabile della protezione dati e incaricati, nuovi obblighi e nuove responsabilità

Mappa dell'argomento:



Responsabilità del titolare del trattamento "Accountability" art. 24 GDPR

L'art. 24 introduce le azioni che deve intraprendere il titolare del trattamento in merito alla propria "accountability", ovvero obbligo di documentazione e analisi dei rischi (*risk based approach*). Si traduce in un principio di responsabilità per il titolare* che si deve tradurre nella dimostrazione di aver adottato un complesso di misure organizzative e tecniche per la protezione dei dati. **Il titolare deve perciò dimostrare proattivamente di aver adottato le misure per un trattamento dei dati conforme al regolamento (efficacia delle misure che nasce da un processo di DPIA *Data Protection Impact Assessment***).**

* Titolare = Persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità ed i mezzi del trattamento di dati personali.

** *Data Protection Impact Assessment* = Valutazione degli impatti privacy del processo aziendale e degli strumenti informatici a supporto.

Questa analisi si traduce in politiche adeguate e proporzionate al trattamento effettuato dal titolare in relazione alla protezione dei dati.

Nell'art. 24 al 3 comma si introduce il concetto di "Codice di condotta" (art. 40) o altri meccanismi di certificazione come elemento per dimostrare il rispetto degli obblighi del titolare. **Ma cosa sono i codici di condotta?** I codici di condotta, destinati a contribuire alla corretta applicazione del GDPR, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese, dovrebbero essere redatti dalle associazioni e dalle organizzazioni che rappresentano categorie di titolari del trattamento o di responsabili del trattamento e dovrebbero tenere conto delle caratteristiche specifiche dei

settori di riferimento, nonché delle diverse esigenze connesse alle dimensioni aziendali, con particolare attenzione alle piccole e medie imprese, **ad oggi non vi sono codici di condotta di riferimento né meccanismi certificatori a** supporto.

Protezione fin dalla Progettazione "Privacy by design" art. 25 GDPR

L'articolo 25, in particolare, introduce il principio di **privacy by design** e **privacy by default**, un approccio concettuale innovativo che impone alle aziende l'obbligo di avviare un progetto prevedendo, fin da subito, gli strumenti a tutela dei dati personali.

Privacy by design

Il concetto di *privacy by design* risale al 2010, già presente negli Usa e Canada e poi adottato nel corso della 32ma Conferenza mondiale dei Garanti privacy.

I principi che reggono il sistema sono i seguenti:

- **prevenire non correggere**, cioè i problemi vanno valutati nella fase di progettazione;
- privacy come impostazione di default;
- privacy incorporata nel progetto;
- massima funzionalità, in maniera da rispettare tutte le esigenze (rifiutando le false dicotomie quali più privacy = meno sicurezza);
- sicurezza durante tutto il ciclo del prodotto o servizio;
- **trasparenza**;
- centralità dell'utente.

Quindi, il sistema di tutela dei dati personali deve porre l'utente al centro, in tal modo obbligando ad una **tutela effettiva da un punto sostanziale, non solo formale**, cioè non è sufficiente che la progettazione del sistema sia conforme alla norma se poi l'utente non è tutelato.

Pro e Contro…
Un approccio *risk based* ha l'evidente vantaggio di pretendere degli obblighi che possono andare oltre la mera conformità alla legge, è sicuramente più flessibile e adattabile al mutare delle esigenze e degli strumenti tecnologici, ma ha anche lo svantaggio di delegare all'azienda la valutazione del rischio, rendendo più difficili le contestazioni in caso di violazioni.

Privacy by default (minimizzazione)
Il principio di *privacy by default* stabilisce, invece, che per impostazione predefinita le imprese dovrebbero trattare solo i dati personali nella **misura necessaria e sufficiente** per le finalità previste e per il **periodo strettamente necessario** a tali fini. Occorre, quindi, progettare il sistema di trattamento di dati garantendo la non eccessività dei dati raccolti (detta anche minimizzazione).

L'introduzione di tali due principi obbliga, ovviamente, le imprese a predisporre una valutazione di impatto privacy ogni volta che avviano un progetto che prevede un trattamento di dati (DPIA).

Precisazioni dal Garante…
Dunque, l'intervento delle autorità di controllo sarà principalmente "ex post", ossia si collocherà successivamente alle determinazioni assunte autonomamente dal titolare; ciò spiega l'abolizione a partire dal 25 maggio 2018 di alcuni istituti previsti dalla direttiva del 1995 e dal Codice italiano (come la notifica preventiva dei trattamenti all'autorità di controllo), sostituiti da obblighi di tenuta di un **registro dei trattamenti** da parte del titolare/responsabile e, appunto, di effettuazione di valutazioni di impatto in piena autonomia.

Responsabile del trattamento art. 28 GDPR

Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a **responsabili del trattamento** che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato. L'art. 28 fissa più dettagliatamente *(rispetto all'art. 29 del Codice)* le **caratteristiche dell'atto con cui il titolare designa un responsabile del trattamento** attribuendogli specifici compiti: deve trattarsi, infatti, di un **contratto** (o altro atto giuridico conforme al diritto nazionale) e deve **disciplinare tassativamente almeno le materie riportate al paragrafo 3 dell'art. 28** al fine di dimostrare che il responsabile fornisce "garanzie sufficienti" – quali, in particolare, la natura, durata e finalità del trattamento o dei trattamenti assegnati, le categorie di dati oggetto di trattamento, le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel regolamento;

- consente la **nomina di sub-responsabili del trattamento** da parte di un responsabile *(si veda art. 28, paragrafo 1)*, per specifiche attività di trattamento;
- prevede **obblighi specifici in capo ai responsabili del trattamento**, in quanto distinti da quelli pertinenti ai rispettivi titolari. Ciò riguarda, in particolare, la tenuta del **registro dei trattamenti** svolti *(ex art. 30, paragrafo 2)*; l'adozione di idonee **misure tecniche e organizzative per garantire la sicurezza** dei trattamenti *(ex art. 32 regolamento)*; la **designazione di un RPD-DPO**, nei casi previsti dal regolamento o dal diritto nazionale *(si veda art. 37 del regolamento)*.

Designazione responsabile della protezione dei dati RGDP – DPO art. 37 GDPR

La designazione del responsabile della protezione dei dati è uno degli obblighi del titolare nei confronti della attività controllo, che verranno sviluppati compiutamente nel prossimo modulo, ma la figura compone la struttura organizzativa per cui se ne anticipa la analisi. L'art. 37 recita al comma 1:

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

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

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.

In merito all'obbligatorietà della nomina si ritorna sempre ai casi in cui il trattamento si riferisca a particolari categorie di dati e, comunque, sempre ai dati riconducibili all'art. 9 del Regolamento (dati sensibili).

Per quanto riguarda l'argomento è intervenuto il WP 29 (WP 243 REV.01) con le Linee Guida sui responsabili della protezione dei dati (RPD) nella versione emendata e adottata in data 5 aprile 2017.
Nella premessa si specifica che, pur non essendo una nomina obbligatoria per chiunque tratti i dati, ma solo in casi particolari, se ne consiglia l'adozione. I RPD non rispondono personalmente in caso di inosservanza del

RGDP in quanto spetta al titolare o al responsabile dimostrare che le operazioni di trattamento dei dati sono conformi al Regolamento (art. 24 Par.1).
Nelle linee guida si specifica la definizione di "Larga Scala" (Vedi WP 29 Linee Guida sul Responsabile della Protezione dei Dati RPD e Linee Guida su DPIA):

- Numero dei soggetti interessati al trattamento in termini assoluti o rispetto alla popolazione di riferimento;
- Volume dei dati e/o le diverse tipologie di dati oggetto del trattamento;
- La durata, ovvero la persistenza del dell'attività di trattamento;
- La portata geografica dell'attività di trattamento.

Lo stesso WP 29 afferma che "in realtà è impossibile precisare la quantità di dati oggetto di trattamento o il numero di interessati in modo da coprire tutte le eventualità, d'altra parte, ciò non significa che sia impossibile col tempo individuare alcuni standard utili a specificare in termini più specifici e/o quantitativi cosa debba intendersi per "larga scala".

Ma che qualità professionali deve avere il RPD?
Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39 (compiti del responsabile).

Anche in questo caso nessuna definizione tassativa…

Posizione e compiti del RPD artt. 38 - 39

Si evidenzia comunque la totale indipendenza e autonomia del soggetto incaricato a ricoprire il ruolo di RPD e anche la posizione di terzietà che assume nella struttura, ivi compreso il profilo della responsabilità che resta in capo al titolare. Il RPD può assumere altri ruoli l'importante è che questi non siano in conflitto d'interesse con la sua figura, deve avere capacità di assolvere ai propri compiti in quanto in possesso di conoscenze e di qualità professionali, inoltre deve possedere libertà di azione.

Le generalità del RPD devono essere comunicate alla pertinenti autorità di controllo e devono essere comunicate a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno della struttura in cui opera.

Naturalmente il RPD dovrà essere coinvolto nelle questioni riguardanti la sicurezza dei dati e che perciò sia presente (o informato) su eventuali meeting del management competente, qualora le decisioni che verranno prese non saranno conformi alle raccomandazioni del RPD se ne dovrà tenere adeguata documentazione. Qualora vi siano violazioni sui dati il RPD dovrà essere tempestivamente informato.

Il titolare dovrà assicurare al RPD la seguente operatività:
_ Supporto attivo nelle decisioni del senior management;
_ Supporto adeguato (infrastrutture e, ove opportuno, personale);
_ Accesso garantito ad altri servizi (risorse umane, ufficio giuridico, IT, sicurezza, ecc.) così da fornire al RPD supporto, informazioni e input essenziali;
_ Alla luce delle dimensioni dell'azienda può risultare utile e necessario costituire un gruppo di lavoro RPD. In casi del genere è opportuno definire con precisione la struttura interna del gruppo di lavoro nonché i compiti e le responsabilità individuali.

I compiti specifici del RPD saranno:
_ Sorvegliare l'osservanza del RGPD;
_ Valutazione d'impatto sulla protezione dei dati (DPIA);
_ Cooperazione con l'autorità di controllo, funzione e punto di contatto;
_ Approccio basato sul rischio (accountability);
_ Realizzazione inventario trattamenti.

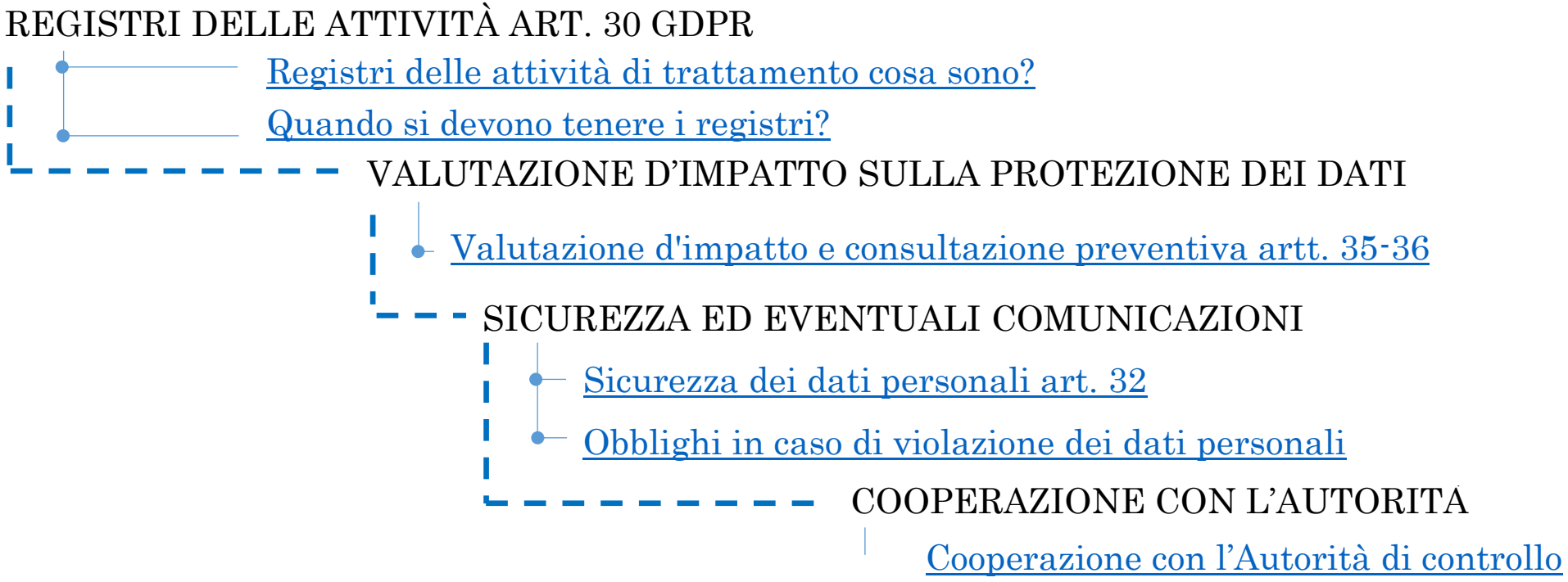
Incaricati artt. 4 punto 10, art. 29 e art. 32 punto 4

In realtà nel regolamento non si parla esplicitamente di incaricati (a differenza del D.lgs. 196 / 2003), se ne fa menzione all'art. 4 punto 10 escludendo dalla definizione di "terzo" il titolare, il responsabile ed i soggetti autorizzati al trattamento dei dati sotto la diretta responsabilità del titolare o del responsabile, una definizione piuttosto allineata al D.lgs. 196 / 2003 e nell'art. 29 (obbligo del responsabile del trattamento) e 32 (obbligo del titolare) che recitano:
Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Questo pare un obbligo alla formazione o, comunque, a fornire le istruzioni agli incaricati al trattamento (così come definito dall'art. 30 del D.lgs.196/2003). Quest'obbligo, pare, non soggiacere a limiti di dimensione aziendale.

4 I nuovi adempimenti del titolare verso l'autorità di controllo

Mappa dell'argomento:



Registri delle attività di trattamento cosa sono?

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

a) Il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
b) Le finalità del trattamento;
c) Le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
d) Ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49 GDPR, la documentazione delle garanzie adeguate;
e) Ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
f) Ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1 GDPR.

Quando si devono tenere i registri?

Il limite dimensionale posto è quello dei 250 dipendenti, oppure del trattamento da parte della struttura dei dati "particolari" descritti all'art. 9 (quelli che si definivano "sensibili" nel D.lgs. 196/2003). Quindi, sicuramente strutture che trattano dati idonei a rivelare stato di salute, studi dentistici, studi psicologici, farmacie, studi commerciali, consulenti del lavoro e avvocati (nonché agenzie assicurative e di viaggio).

Valutazione d'impatto e consultazione preventiva artt. 35-36

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

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

Il titolare del trattamento, quando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.

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

a) Una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;

b) Il trattamento, su **larga scala**, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;

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

La valutazione contiene almeno:

a) Una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, 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 per i diritti e le libertà degli interessati di cui al paragrafo 1; e

d) Le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

La DPIA è uno strumento importante in termini di responsabilizzazione (*accountability*), in quanto aiuta il titolare non soltanto a rispettare le prescrizione del RGPD, ma anche a dimostrare l'adozione di misure idonee a garantire il rispetto di tali prescrizioni (si veda anche l'art. 24).

In pratica la DPIA è una procedura che permette di realizzare e dimostrare la conformità con le norme!

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.

Linee Guida DPIA e criteri per stabilire se un trattamento presenti "Rischio Elevato" (WP 29)

Innanzi tutto le linee guida esprimono un concetto importante ed impattante per gli attori:
"La semplice circostanza per cui non si presentino le condizioni che generino l'obbligo di condurre la DPIA non riduce in alcun modo l'obbligo più generale cui soggiacciono i titolari di mettere in atto misure finalizzate a gestire in modo idoneo i rischi per i diritti e le libertà degli interessati."

In pratica significa valutare in modo continuativo i rischi creati dalle proprie tipologie di trattamenti così da poter eventualmente individuare quelli che possono presentare rischi.

Oggetto della DPIA

Come visto l'oggetto della DPIA può essere un trattamento od un insieme di trattamenti che possano avere caratteristiche simili. Quali sono le analogie che rendono i trattamenti simili?
_ Natura del trattamento;
_ Ambito di trattamento;
_ Contesto in cui viene effettuato il trattamento;
_ Finalità del trattamento;
_ Rischi derivanti dal trattamento.
Nella pratica non occorre svolgere una nuova DPIA per quei trattamenti già oggetto di analisi (per esempio una Compagnia Ferroviaria – titolare del trattamento, che abbia già svolto la DPIA sui propri impianti di videosorveglianza nelle stazioni e che, aprendone una nuova, attivasse un nuovo impianto).

Quali trattamenti sono soggetti a DPIA?

In generale una DPIA si deve condurre quando il trattamento possa presentare "rischio elevato"

Intanto viene specificato che si tratta di un requisito pertinente quando si abbia a che fare con una tecnologia di trattamento innovativa. L'elenco che abbiamo presentato al Paragrafo 1 dell'art. 35 è per definizione non esaustivo, il WP 29 indica 9 criteri di giudizio:

1_ Trattamenti valutativi o di "*scoring*" (tipo rischio creditizio, data base per lotta alle frodi, creazione di profili comportamentali o di marketing a partire dalle navigazioni compiute sul web…);

2_ Decisioni automatizzate che producono effetti giuridici significativi derivanti da profilazione;

3_ Monitoraggio sistematico derivante da attività di videosorveglianza;

4_ **Dati sensibili o di natura estremamente personale:** si tratta dei dati personali di cui all'art. 9 oltre che i dati personali relativi a condanne penali o reati di cui all'art. 10. Ma qui, il WP 29 afferma una cosa di estremo interesse: "Al di là di queste disposizioni del Regolamento, vi sono categorie di dati che possono aumentare i rischi eventuali per i diritti e le libertà delle persone fisiche. Si tratta di dati considerati sensibili (**nell'accezione comune del termine**) in quanto connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche…), o quando incidano su di un esercizio di un diritto fondamentale (come dati relativi alla ubicazione che non permettono un libero spostamento) oppure dati che potrebbero comportare un grave danno sulla vita quotidiana (quali dati su transazioni finanziarie che potrebbero essere usati per frodi)."

5_ Per Larga Scala si rimanda alla definizione fatta per la designazione del DPO;

6_ Combinazioni o raffronto di insiemi di dati, per esempio derivanti da due o più trattamenti svolti per finalità diverse e/o da titolari distinti secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;

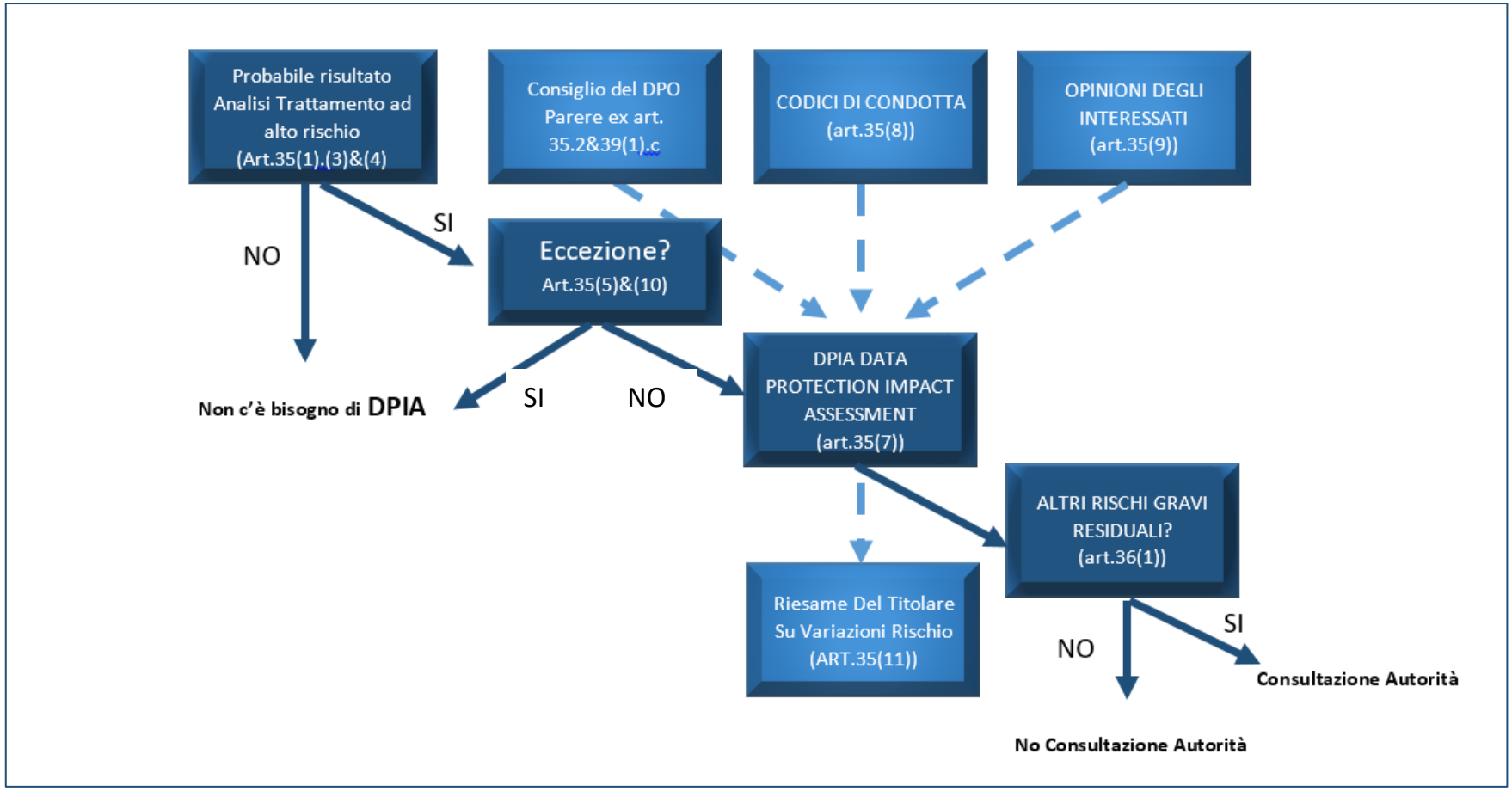
7_ Dati relativi a interessati vulnerabili, quando per l'interessato non può essere così semplice non acconsentire od opporsi al trattamento né può esercitare con facilità i propri diritti. In questo caso il WP 29 indica precise categorie come soggetti con patologie psichiatriche, richiedenti asilo, anziani e anche pazienti.
8_ Utilizzi innovativi o di nuove soluzioni tecnologiche o organizzative, come ad esempio il riconoscimento biometrico per dare accesso a determinati luoghi fisici;
9_ Tutti quei trattamenti che di per sé "impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto".

Principio "statistico":
Il WP 29 indica che quando sussistano almeno **due criteri** di quelli elencati relativamente ad un certo trattamento un titolare sia chiamato ad effettuare la DPIA. Tuttavia in taluni casi il titolare può decidere che se anche uno solo di questi criteri sussista si debba procedere alla DPIA.
Al contrario un titolare che si trovasse ad effettuare trattamenti che rispondano ai criteri ma che considerasse il trattamento non a rischio elevato può non effettuare la DPIA a patto che:
_ Venga annotato il motivo che porta a tale decisione;
_ Venga verbalizzata l'opinione del DPO.
Ricordiamoci poi che il GDPR prevede che l'autorità di controllo renda pubblico l'elenco di trattamenti soggetti alla valutazione d'impatto (art. 35 co. 4) e quelli non soggetti (art. 35 co. 6).

È obbligatorio pubblicare la DPIA? No, ma pubblicarne una sintesi può favorire un rapporto fiduciario e la si deve inviare in forma completa all'autorità di controllo in caso di consultazione preventiva ovvero su richiesta dell'autorità stessa.

Processo iterativo relativo ad una DPIA:

Schema DPIA


Probabile risultato Analisi Trattamento ad alto rischio (Art.35(1).(3)&(4)
Consiglio del DPO Parere ex art. 35.2&39(1).c
CODICI DI CONDOTTA (art.35(8))
OPINIONI DEGLI INTERESSATI (art.35(9))
SI
NO
Eccezione? Art.35(5)&(10)
Non c'è bisogno di DPIA
SI
NO
DPIA DATA PROTECTION IMPACT ASSESSMENT (art.35(7))
ALTRI RISCHI GRAVI RESIDUALI? (art.36(1))
Riesame Del Titolare Su Variazioni Rischio (ART.35(11))
NO
SI
Consultazione Autorità
No Consultazione Autorità

Sicurezza dei dati personali art. 32

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) La pseudonimizzazione e la cifratura dei dati personali;

b) La capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) La capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) Una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.

4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Al punto 4 si riporta pedissequamente l'art 29 (ridondanza?) e comunque si ribadisce l'obbligo della formazione e dell'istruzione ai dipendenti, su cosa? Intanto sul livello di misure di sicurezza tecniche e organizzative adeguate al contesto per garantire un livello di sicurezza in relazione alla integrità dei dati e alla possibilità che vi siano accessi non autorizzati. Quindi, fra le altre, si dovrà implementare una procedura di verifica dello stato delle misure di sicurezza per testarne, verificarne e valutarne l'efficacia.

Si dovranno perciò comprendere quali siano le azioni da intraprendere, come riportarle al titolare e come disciplinare eventuali azioni correttive, una sorta di modello organizzativo.

Obblighi in caso di violazione dei dati personali

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

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

a) Descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

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

c) Descrivere le probabili conseguenze della violazione dei dati personali;

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

4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

CD Data Breach, ovvero l'obbligo di comunicare all'Autorità eventi che abbiano comportato fisicamente o potenzialmente danni ai dati personali recando così pregiudizio ai diritti degli interessati
Per ora i casi esaminati sono relativi a società private nell'ambito delle telecomunicazioni, a particolari trattamenti sanitari (biometrie e dossier sanitario elettronico), nonché alla PA.

Comunicazione di una violazione dei dati personali all'interessato

1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

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

3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura (…).

Cooperazione con l'Autorità di controllo

Il titolare del trattamento, il responsabile del trattamento e, ove applicabile, il loro rappresentante cooperano, su richiesta, con l'autorità di controllo nell'esecuzione dei suoi compiti.

5 Trasferimento verso paesi terzi ed organizzazioni internazionali (cenni)

L'art. 44 del GDPR sancisce che "Qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni di cui al presente capo, fatte salve le altre disposizioni del presente regolamento. Tutte le disposizioni del presente capo sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal presente regolamento non sia pregiudicato."

Ad oggi l'elenco dei paesi è disciplinato dall'art. 25 Co.1 della Direttiva 95/46/CE, a meno che il Paese in questione garantisca un livello di protezione "adeguato"; la Commissione ha il potere di stabilire tale adeguatezza attraverso una specifica **decisione** (articolo 25, comma 6, della Direttiva 95/46/CE). In tal caso il trasferimento non necessita di autorizzazioni specifiche.

6 Sistema sanzionatorio e diritto al risarcimento, responsabilità del titolare.

Mappa dell'argomento:

DIRITTO AL RISARCIMENTO E RESPONSABILITÀ ART. 82 GDPR

- Diritto al risarcimento e responsabilità

CONDIZIONI GENERALI PER INFLIGGERE SANZIONI

- Condizioni generali per infliggere sanzioni amministrative art. 83

SANZIONI

- Sanzioni art.83 segue…

Diritto al risarcimento e responsabilità

1. Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.
2. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.
3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile.
4. Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.
5. Qualora un titolare del trattamento o un responsabile del trattamento abbia pagato, conformemente al paragrafo 4, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno conformemente alle condizioni di cui al paragrafo 2.

Condizioni generali per infliggere sanzioni amministrative art. 83

(Par. 2) Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi:

b) Il carattere doloso o colposo della violazione;

c) Le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;

d) Il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32;

e) Eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;

f) Il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;

g) Le categorie di dati personali interessate dalla violazione;

h) La maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;

i) Qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;

j) L'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42; e

k) Eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

Sanzioni art.83 (segue…)

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

4. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 10 000 000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

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

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

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

5. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

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

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

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

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

e) L'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1.

6. In conformità del paragrafo 2 del presente articolo, l'inosservanza di un ordine da parte dell'autorità di controllo di cui all'articolo 58, paragrafo 2, è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.