STUDIO NICOLAZZO

Business Tax Legal Consulting

IL REGOLAMENTO EUROPEO 679/2016 (General Data Protection Regulation – GDPR)

RELATORE: ***Prof. Pasquale Nicolazzo***

MULTIBUSINESS s.r.l.
Via C. Colombo 40 - 88046 Lamezia T.
E-mail: p.nicolazzo@multibusiness.it

CEO: Dott. Pasquale Nicolazzo – **P.IVA**: 03696180797
Sede legale: Via Melia 37 – 88040 Feroleto A. (CZ)
Sede operativa: Via Roma 120 - 20010 Bareggio (MI)
PEC: info@pec.studionicolazzo.it - Email: info@studionicolazzo.it

ARTIGIANCASSA Point
GRUPPO BNP PARIBAS
Via S. Giorgio 18/2, 88040 Serrastretta
Email: segreteria@studionicolazzo.i

REGOLAMENTO EUROPEO
- GDPR -

È formato da 179 Considerando e da 99 Articoli che mirano ad adeguare la protezione dei dati rispetto all'evoluzione tecnologica che ha determinato un aumento dei sistemi informatici e dei flussi

COS'È IL GDPR? QUAL È LA SUA IMPORTANZA?

È la normativa europea in materia di protezione dei dati personali.

Il suo scopo è la definitiva armonizzazione della regolamentazione in materia di protezione dei dati personali all'interno dell'Unione Europea

Trattandosi di un Regolamento Europeo, non necessita di recepimento da parte degli Stati dell'Unione e sarà attuato allo stesso modo in tutti gli Stati membri.

Qual è la differenza tra Direttiva UE e Regolamento UE?

REGOLAMENTO UE: ha portata generale (non si rivolge a soggetti determinati, ma pone delle norme generali e astratte), è obbligatorio in tutti i suoi elementi (nel senso che non può essere applicato solo parzialmente), e, infine, è direttamente applicabile in ciascuno degli Stati membri (non è quindi necessario un atto dello Stato membro che ne permetta l'esecuzione)

DIRETTIVA UE: ha come destinatari gli Stati membri (e quindi non tutti i soggetti giuridici dell'UE). Lo Stato ha "obbligo di risultato", cioè l'obbligo di raggiungere quel determinato obiettivo entro il termine fissato dalla direttiva stessa, ma si lascia libertà allo Stato per quanto riguarda i mezzi con cui conseguirlo (cioè tramite una legge, un regolamento o anche semplicemente mediante comportamenti dell'amministrazione pubblica).

Evoluzione normativa

Direttiva Europea 24/10/1995 95/46/CE -
Recepita in Italia dalla L. 31/12/1996 n. 675

Carta di Nizza (2000)

Direttiva Europea 2002/58/CE –
D.Lgs. 30 Giugno 2003 n. 196 "Codice in materia di protezione dei dati personali"

Trattato di Lisbona (2009)

Regolamento Europeo 679/2016 "GDPR» - G.U. 4/5/2016

Vengono dati 2 anni di tempo per l'applicazione effettiva

Il Regolamento sostituisce (non integralmente) il D.Lgs. n. 196/2003 (c.d. Codice Privacy)

EVOLUZIONE TEMPORALE DELLA NORMA

1997

Legge 31 dicembre 1996, n. 675 “Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali ”

2003

DECRETO LEGISLATIVO 30 giugno 2003, n.196 recante il “Codice in materia di protezione dei dati personali”

2016

REGOLAMENTO EUROPEO del 27 aprile 2016, n. 679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali

2018

DECRETO LEGISLATIVO **10 agosto** 2018, n. 101, recante “ Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679

- **DGR 1947/2003** - L. 675/96 "TUTELA DEI DATI PERSONALI". INDIVIDUAZIONE TITOLARE TRATTAMENTI REGIONE BASILICATA - GIUNTA REGIONALE E DISPOSIZIONI IN MERITO AI RESPONSABILI DEI TRATTAMENTI MEDESIMI. REVOCA DRIBERAZIONE G.R. n. 9069/97.

- **DGR 2143/2003** - L. 31 DICEMBRE 1996, N.675 •TUTELA DELLE PERSONE E DEGLI ALTRI SOGGETTI RISPETTO AL TRATTAMENTO DEI DATI PERSONALI• - NOMINA RESPONSABILI.

AMBITO DI APPLICAZIONE MATERIALE

Il GDPR si applica:

- ☒ alle persone fisiche e al trattamento interamente o parzialmente automatizzato dei dati personali e al trattamento non automatizzato di dati contenuti in archivio o destinati a figurarvi.

Non si applica, invece:

- ☐ ai trattamenti effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;
- ☐ ai dati anonimi.

DISPOSIZIONI GENERALI: ESCLUSIONI

- IL GDPR non si applica per il Trattamento dei dati personali effettuato:

- PER **ATTIVITÀ CHE NON RIENTRANO NELL'AMBITO DI APPLICAZIONE DEL DIRITTO DELL'UE** EFFETTUATO DAGLI STATI MEMBRI NELL'ESERCIZIO DI ATTIVITÀ RELATIVE ALLA **POLITICA ESTERA** E DI **SICUREZZA NAZIONALE O COMUNE DELL'UE**

- effettuato dalle autorità competenti a fini di **prevenzione, indagine, accertamento o perseguimento di REATI O ESECUZIONE DI SANZIONI PENALI** incluse la **salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.**

DEFINIZIONI

ARCHIVIO

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,

Il GDPR si applica al trattamento automatizzato o non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.

DATO PERSONALE

Art. 4, par. 1 del GDPR

Qualsiasi informazione riguardante una persona fisica identificata o identificabile (c.d. «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

Art. 9, par. 1 del GDPR

Dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare 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.

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

«Dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

«Dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

DATI RELATIVI A CONDANNE PENALI E REATI

Art. 10, par. 1 del GDPR

Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.

Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.

MA COSA SI INTENDE PER TRATTAMENTO?

Art. 4, par. 1 del GDPR

Con il termine «Trattamento» si indica qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione,

I PRINCIPI DEL GDPR

Il Regolamento impone il rispetto dei seguenti Principi:

LICEITA', CORRETTEZZA E TRASPARENZA

LIMITAZIONE DELLE FINALITA':

Determinate, esplicite e legittime

MINIMIZZAZIONE DEI DATI:

Adeguati, pertinenti e limitati

ESATTEZZA:

i Dati devono essere Esatti e, se necessario, aggiornati

LIMITAZIONE DELLA CONSERVAZIONE:

Per un periodo temporale limitato al conseguimento delle finalità

INTEGRITA' E RISERVATEZZA:

Deve essere garantita un'adeguata sicurezza dei dati personali

RESPONSABILIZZAZIONE:

il Titolare è tenuto a comprovare il rispetto di tali principi

PRINCIPI APPLICABILI AL TRATTAMENTO

Parte 1

I dati personali sono:

- ✓ trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (**liceità, correttezza e trasparenza**);
- ✓ raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali (**limitazione della finalità**);
- ✓ conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (**limitazione del periodo di conservazione**);

PRINCIPI APPLICABILI AL TRATTAMENTO

Parte 2

I dati personali sono:

- ✓ adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (**minimizzazione dei dati**);
- ✓ esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (**esattezza**);
- ✓ trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (**integrità e riservatezza**).

Liceità e Basi giuridiche del trattamento

IL TRATTAMENTO È LECITO SOLO SE E NELLA MISURA IN CUI RICORRE ALMENO UNA DELLE SEGUENTI CONDIZIONI:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;
f)il trattamento è necessario per il perseguimento del legittimo interesse del Titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in articolare se l'interessato è un minore.

GDPR

Articolo 9 - Trattamento di categorie particolari di dati personali

Il General Data Protection Regulation non parla di dati sensibili ma di **DATI PARTICOLARI** e all'articolo 9 recita: "È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare 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." Il divieto non si applica in presenza di **consenso esplicito** o di **necessità** per assolvere gli obblighi.

Articolo 10 - Trattamento dei dati personali relativi a condanne penali e reati

Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, **deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri** che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.

Articolo 9, paragrafo 2, del GDPR

1. Consenso espresso (lettera a)
2. Diritto del lavoro, sicurezza sociale, protezione sociale (lettera b)
3. Tutela degli interessi vitali (lettera c)
4. Organizzazioni a orientamento politico, ideologico, religioso e sindacale (lettera d)
5. Dati auto-pubblicati (lettera e)
6. Reclami legali e azioni legali (lettera f)
7. Interesse pubblico significativo (lettera g)
8. Settore sanitario e sociale (lettera h)

Assistenza sanitaria, Medicina del lavoro, Valutazione della capacità lavorativa di un dipendente, diagnostica medica, Assistenza o trattamento nel settore sanitario o sociale, Gestione di sistemi e servizi nel settore sanitario o sociale

9. Salute pubblica (lett. I)
10. Archiviazione, ricerca e finalità statistiche (lettera j)

PRINCIPIO DI «ACCOUNTABILITY»

Parte 1

DEFINIZIONE SECONDO IL GDPR

[…] *Art. 5, par. 2 del GDPR*

Il Titolare del trattamento è competente per il rispetto dei principi previsti dal GDPR e in grado di comprovarlo (c.d principio di «***Responsabilizzazione***»).

Considerando 74: "Il Titolare del trattamento è tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente Regolamento, compresa l'efficacia delle misure. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche".

Il principio di «***Accountability***», nell'accezione inglese appunto «Responsabilizzazione», impone un cambio culturale, un diverso approccio alla *Privacy*, che deve essere non più formale ma sostanziale

PRINCIPIO DI «ACCOUNTABILITY»

Parte 2

In sostanza viene affidato al Titolare del trattamento il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali nel rispetto delle disposizioni normative. Il Titolare dovrà saper dimostrare, con ragionamento logico, l'adozione di comportamenti proattivi e tali da dimostrare la concreta attuazione di misure finalizzate ad assicurare l'applicazione del regolamento.

IL TITOLARE HA L'OBBLIGO DI DIMOSTRARE L'ADOZIONE DI:

- misure tecniche per la sicurezza fisica e informatica dei dati;
- misure organizzative inerenti politiche e procedure interne, FORMAZIONE DEL PERSONALE, verifiche e adeguamenti costanti;
- un sistema documentale che comprovi tali misure;

PRIVACY BY DESIGN

Art. 25, par. 1 del GDPR

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il Titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la ***pseudonimizzazione***, volte ad attuare in modo efficace i principi di protezione dei dati, quali la ***minimizzazione***, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

PRIVACY BY DESIGN INTESA COME PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE

- Impone di esaminare e configurare il trattamento dei dati prevedendo fin dall'inizio le garanzie previste dal Regolamento per tutelare i diritti degli interessati.

Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio e richiede un'analisi preventiva e un impegno da parte dei Titolari che devono attivarsi in una serie di attività specifiche e dimostrabili.

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

PRIVACY BY DEFAULT

Art. 25, par. 2 del GDPR

Il Titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Tale principio intende indicare che i sistemi di raccolta dei dati devono essere configurati in modo da non consentire trattamenti diversi da quelli previsti nella progettazione

PRIVACY BY DEFAULT INTESA COME PROTEZIONE DEI DATI PER IMPOSTAZIONE PREDEFINITA

Il principio della «Privacy by Default» stabilisce che per impostazione predefinita:

- siano trattati solo i dati personali necessari per ogni specifica finalità del trattamento;
- non possano essere trattati dati personali ulteriori rispetto a quelli minimi indispensabili per ogni specifica finalità (***principio della minimizzazione***)
- venga garantito che i dati raccolti non siano conservati per tempi ulteriori rispetto a quelli minimi necessari

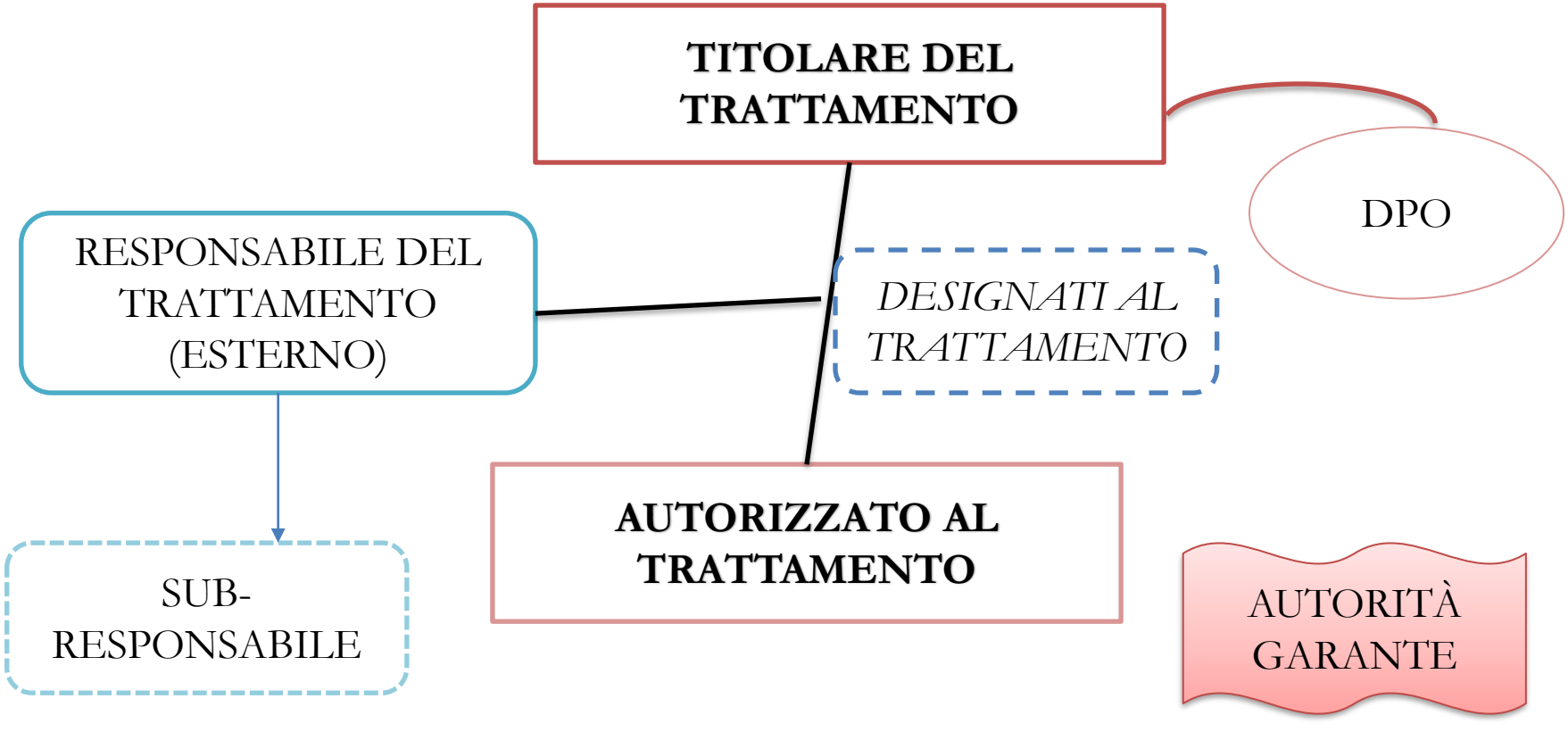
ACCOUNTABILITY
PRIVACY BY DESIGN
PRIVACY BY DEFAULT

Riassumendo, questi principi promuovono un'idea di protezione dei dati nuova e più tecnologica, incentrata sulla responsabilizzazione di tutti gli addetti al trattamento.

Una protezione dei dati più tecnologica perché richiede la progettazione e l'adozione di misure tecniche e organizzative, di procedure e di strumenti adeguati al trattamento dei dati personali.

Dalla forma alla sostanza

I RUOLI PREVISTI DAL GDPR



TITOLARE DEL TRATTAMENTO

Art. 4, par. 1 del GDPR

La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri

CONTITOLARI DEL TRATTAMENTO

Art. 26, par. 1 del GDPR

Allorché due o più Titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono Contitolari. Determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni.

RESPONSABILE DEL TRATTAMENTO

Artt. 4 par. 1 – 28 par. 1 – 28 par. 3 del GDPR

La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento

[…]

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

[…]

I trattamenti da parte di un Responsabile sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il Responsabile al Titolare e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del Titolare

OBBLIGHI DEL RESPONSABILE DEL TRATTAMENTO

- ✓ Trattare i dati personali soltanto su istruzione documentata del Titolare del trattamento;
- ✓ Garantire che le persone Autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- ✓ Adottare le adeguate misure di sicurezza;
- ✓ Rispettare i limiti previsti per la nomina dei sub-Responsabili;
- ✓ Assistere il Titolare in relazione all'esercizio dei diritti degli interessati;
- ✓ Cancellare o restituire al Titolare tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti;
- ✓ Mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di legge e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzati dal Titolare del trattamento o da un altro soggetto da questi incaricato.

.

Ricorso ad un sub-Responsabile del trattamento

Sempre l'articolo 28 del GDPR narra:

"Il Responsabile del trattamento non ricorre a un altro Responsabile senza previa autorizzazione scritta, specifica o generale, del Titolare del trattamento. Nel caso di autorizzazione scritta generale, il Responsabile del trattamento informa il Titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri Responsabili, dando così al Titolare l'opportunità di opporsi".

Viene istituita, così, la figura del sub-Responsabile. Dunque se il Responsabile è scelto direttamente dal Titolare, è quindi possibile che la responsabilità venga in seguito «ripartita», anche se rimane "**l'opportunità di opporsi**". Il Responsabile, designato dal Titolare, dunque, dovrà sempre informare il Titolare stesso di eventuali sostanziali modifiche.

In generale il sub-Responsabile avrà gli stessi obblighi e lo stesso rapporto di subordinazione del Responsabile, e indirettamente opererà per conto del Titolare.

.

TRATTAMENTO SOTTO L'AUTORITÀ DEL TITOLARE DEL TRATTAMENTO

Artt. 4 par. 10 – 29 del GDPR

«Il Responsabile del trattamento, o chiunque agisca sotto l'autorità del Titolare del trattamento, che abbia accesso a dati personali, non può trattare tali dati se non è istruito in tal senso dal Titolare stesso»

Il GDPR non prevede la figura dell'incaricato ma fa riferimento a persone autorizzate al trattamento dei dati sotto l'autorità diretta del Titolare o del Responsabile. L'Autorizzato, è il soggetto PERSONA FISICA che effettua materialmente le operazioni di trattamento sui dati personali. L'autorizzato può operare alle dipendenze del Titolare, ma anche del responsabile se nominato. Ovviamente gli autorizzati possono essere organizzati con diversi livelli di delega.

È fondamentale fornire agli Autorizzati le istruzioni operative, compreso gli obblighi inerenti le misure di sicurezza, e che sia fornita loro la necessaria formazione. In caso contrario, infatti, anche in presenza di formali designazioni, queste sarebbero del tutto prive di valore.

Art. 2-quaterdecies Nuovo Codice Privacy – D.lgs 196/2003 aggiornato al D.lgs 101/2018

Attribuzione di funzioni e compiti a soggetti designati:

1. Il Titolare o il Responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.

2. Il Titolare o il Responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.

RESPONSABILE PROTEZIONE DATI - DPO

Artt. 37 e ss del GDPR

«Il Titolare designa sistematicamente un DPO ogniqualvolta:
a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni;
b) le attività principali del Titolare 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 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

- Il DPO 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 propri compiti.
- Il DPO può essere un dipendente del Titolare oppure assolvere i suoi compiti in base a un contratto di servizi

OBBLIGO DI NOMINA DELLA FIGURA DEL DPO

Amministrazioni ed enti pubblici, fatta eccezione per le autorità giudiziarie;

Tutti i soggetti la cui attività principale consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il monitoraggio regolare e sistematico degli interessati SU LARGA SCALA;

Tutti i soggetti la cui attività principale consiste nel trattamento, su larga scala, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici o di dati relativi a condanne penali.

I COMPITI DEL DPO

Informare e consigliare il titolare o il responsabile del trattamento, nonché i dipendenti, in merito agli obblighi derivanti dal Regolamento e da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

Verificare l’attuazione e l’applicazione del Regolamento nonché delle politiche del titolare o del responsabile del trattamento in materia di protezione dei dati personali, inclusi l’attribuzione delle responsabilità, la formazione del personale coinvolto nelle operazioni di trattamento, e gli audit relativi;

Fornire, se richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliare i relativi adempimenti;

Fungere da punto di contatto per gli interessati;

Cooperare e fungere da punto di contatto per l’Autorità di controllo

TRASPARENZA

Art. 12 del GDPR

Il Titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.

Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato

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

.

INFORMATIVA

Artt. 13 e 14 del GDPR

Vi sono due ipotesi diverse di informativa a seconda che i dati siano o meno raccolti presso l'interessato

Art. 13

Informazioni che il Titolare deve fornire all'interessato qualora i dati personali siano raccolti presso di lui.

Art. 14

Informazioni da indicare ove i dati non siano raccolti presso l'interessato. Esse devono essere fornite entro un tempo ragionevole dall'ottenimento dei dati personali e, al più tardi, entro un mese.

.

ELEMENTI ESSENZIALI

Il Titolare dovrà fornire almeno le seguenti informazioni relative al trattamento:

• L'identità e i dati di contatto del Titolare del trattamento e del DPO (ove applicabile) per le comunicazioni relative all'esercizio dei diritti.
• La descrizione delle finalità per cui viene posto in essere il trattamento.
• I destinatari del trattamento dei dati personali
• Il Periodo di conservazione dei dati personali (ove quantificabile)
• L'intenzione del Titolare di trasferire i dati personali in Paese Extra UE, solo quando esistono nei confronti dei paesi garanzie adeguate di rispetto della
• La specifica e chiara indicazione dei diritti di revoca del consenso, di accesso, di rettifica, di cancellazione, di limitazione, di portabilità dei dati e di opposizione
• Il diritto di proporre reclamo all'Autorità di Controllo «Garante per la protezione dei dati personali»

CONSENSO

Art. 4 par. 1 del GDPR

«Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento»

La richiesta di consenso va presentata in modo chiaramente distinguibile, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro.

• L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca non pregiudica la liceità del trattamento basata sul consenso prima della revoca.

• Particolari condizioni sono poi dettate dall'art.8 del Regolamento nell'interesse dei minori il quale chiarisce che il trattamento di dati personali di minori al di sotto dei 16 anni, o, se previsto dal diritto degli Stati membri, di un'età inferiore ma non al di sotto di 13 anni, è lecito soltanto se e nella misura in cui tale consenso è espresso o autorizzato dal titolare della responsabilità genitoriale sul minore.

REGISTRO DEI TRATTAMENTI

Art. 30 del GDPR

Ogni Titolare del trattamento tiene un Registro in cui sono riportate 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 e del DPO;

b) le finalità del trattamento;

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

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

e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;

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

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative

DIRITTI DELL'INTERESSATO ARTT. 12 A 23

Non si applica: Trattamenti necessari per adempimento obblighi di legge / interesse pubblico / ambito sanitario / ricerca (v. Art. 17, paragrafo 3)

Diritto di accesso (art.15)

- Il diritto di accesso prevede in ogni caso il diritto di ricevere **una copia** dei dati personali oggetto di trattamento.

-Tra le **informazioni da fornire**: il periodo di conservazione previsto o, se non è possibile, i criteri utilizzati per definire tale periodo

- Obbligo di definire una *Data Retention Policy* (ove già non definita) nonché le garanzie applicate in caso di trasferimento dei dati verso Paesi terzi (Attenzione a eventuali provider in outsourcing stabiliti in Paesi extra-Ue!)

-I Titolari possono consentire agli interessati di consultare direttamente, da remoto e in modo sicuro, i propri dati personali (Considerando 68).

Diritto di rettifica (art.16)

- **Cosa**: Rettifica di dati inesatti + Integrazione dati incompleti (tenendo conto della finalità del trattamento)

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

Diritto di cancellazione (diritto all'oblio) (art. 17)

Il diritto all'oblio si configura come un **diritto alla cancellazione** dei propri dati personali **in forma rafforzata**.

a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

b) l'interessato revoca il consenso su cui si basa il trattamento e se non sussiste altro fondamento giuridico per il trattamento;

c) l'interessato si oppone al trattamento;

d) i dati personali sono stati trattati illecitamente;

e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato;

f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione.

Non si applica: Trattamenti necessari per adempimento obblighi di legge / interesse pubblico / ambito sanitario / ricerca

Diritto di limitazione del trattamento (art. 18)

L'interessato ha il diritto di ottenere dal Titolare la limitazione del trattamento quando ricorre una delle seguenti ipotesi:

a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al Titolare per verificare l'esattezza di tali dati personali;
b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
c) benché il Titolare non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
d) l'interessato si è opposto al trattamento in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del Titolare del trattamento rispetto a quelli dell'interessato.

Diritto alla portabilità dei dati (art.20)

- È un nuovo diritto che **non si applica ai trattamenti non automatizzati** (quindi **non** si applica agli archivi o registri cartacei)
- In particolare, sono portabili **solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato** (quindi ***non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'adempimento di obblighi di legge del Titolare***, né ai trattamenti per scopi di ***archiviazione nel pubblico interesse*** per esempio), e solo i dati che siano stati **"forniti" dall'interessato** al Titolare
- Il Titolare deve essere in grado di trasferire direttamente i dati portabili a un altro Titolare indicato dall'interessato, se tecnicamente possibile (**interoperabilità** dei formati).

Tutela amministrativa/giudiziaria

-Art. 77 del Regolamento UE 679/2016 (diritto di proporre «reclamo» alla autorità di controllo competente, cioè al Garante Privacy per quanto riguarda i trattamenti svolti da «soggetti pubblici» o «Autorità pubbliche»

Modalità per l'esercizio dei diritti: sotto il segno della *accountability* e della maggiore efficacia

Le modalità per l'esercizio dei diritti da parte degli interessati sono agli **artt. 11 e 12 del GPDR**.

- Il Titolare del trattamento deve ***agevolare l'esercizio*** dei diritti da parte dell'interessato, adottando idonee *misure (tecniche e organizzative)*.

- Il Titolare deve **fornire riscontro** (artt. **15-22**), e il Responsabile è tenuto a collaborare con il Titolare (art. 28, paragrafo 3, lettera e)

- L'esercizio dei diritti è *gratuito per l'interessato*, ma vi sono eccezioni.

- Il Titolare ha il diritto di chiedere informazioni per identificare l'interessato, secondo modalità idonee (art. 11, paragrafo 2 e art. 12, paragrafo 6).

Il termine per la risposta all'interessato è di **un mese**, anche in caso di diniego, estendibili fino a **tre mesi** in caso di particolare complessità.

Una risposta deve essere fornita in ogni caso (anche se negativa o interlocutoria): artt. 12.3 + 12.4

In caso di richieste manifestamente infondate o eccessive (anche ripetitive) (art. 12.5) il Titolare può stabilire se, e quanto, chiedere come contributo, ovvero se sono chieste più "copie" dei dati personali nel caso del diritto di accesso (art. 15.3), tenendo conto dei costi amministrativi sostenuti.

In ogni caso il **contributo spese** deve essere «ragionevole» (art. 12.5)

VIOLAZIONE DEI DATI PERSONALI «DATA BREACH»

Art. 33 par.1 del GDPR

È la violazione della sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati

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

ADEMPIMENTI

La notifica deve contenere almeno:

- 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;
- 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;
- descrivere le probabili conseguenze della violazione dei dati personali;
- 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.

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

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI – DPIA

Art. 35 e ss del GDPR

Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento effettua, prima di procedere al trattamento, una Valutazione dell'Impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi

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
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.

Il Titolare del trattamento dovrebbe essere responsabile dello svolgimento di una DPIA per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio. Laddove la DPIA 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**

ADEMPIMENTI PER LA SICUREZZA:

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 mette in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

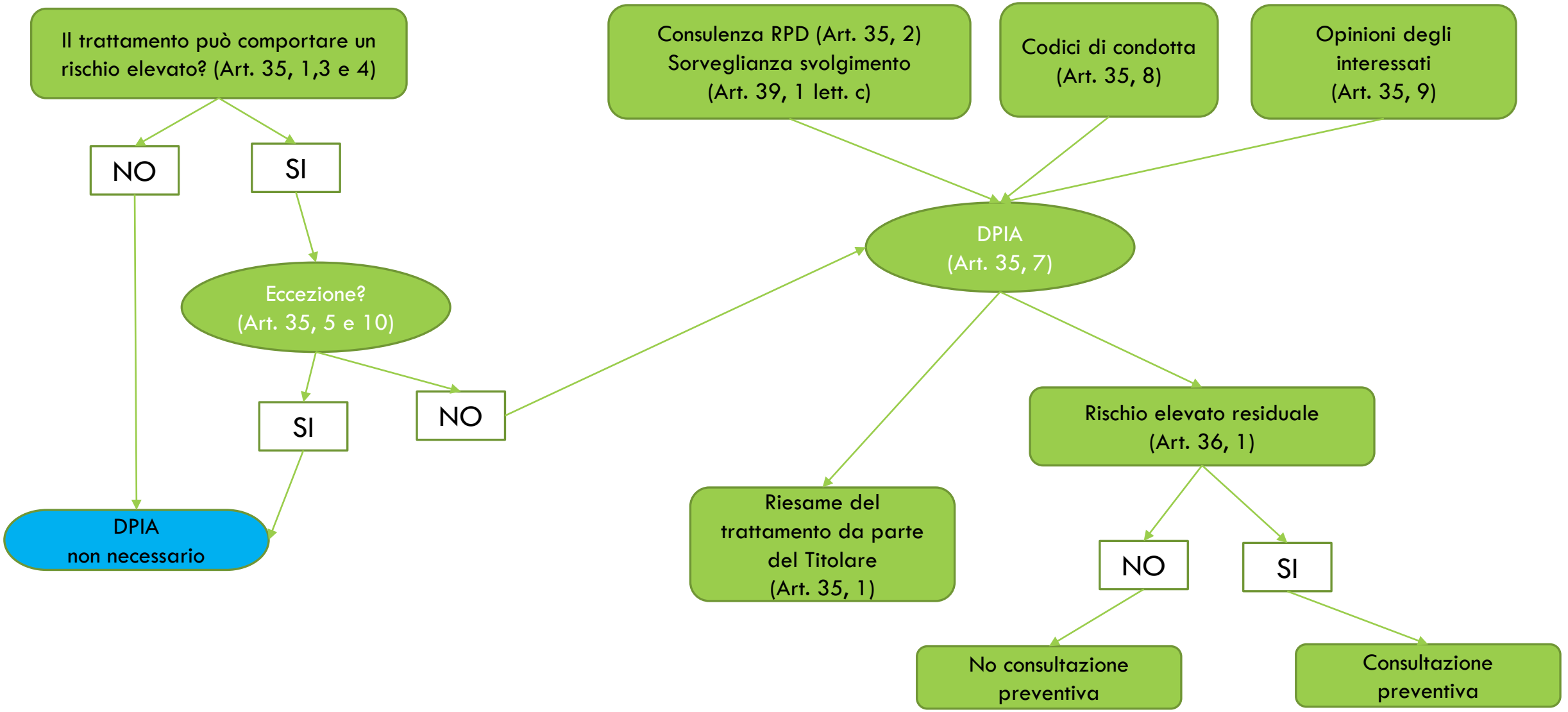
a) la pseudonimizzazione e la cifratura dei dati personali;

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.

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI – QUANDO EFFETTUARLA ?



I codici di condotta e le certificazioni per la protezione dei dati

L'adesione a un Codice di condotta approvato o a un meccanismo di certificazione approvato può essere utilizzata come elemento per dimostrare la conformità dei trattamenti al Regolamento anche con specifico riferimento agli aspetti di sicurezza.

Codici di condotta o certificazioni come strumenti a disposizione dei Titolari (e dei Responsabili) del trattamento per attestare la conformità ai requisiti del Regolamento.

IL SISTEMA SANZIONATORIO

Il GDPR definisce un impianto sanzionatorio molto più rigido di quello previsto dal Codice Privacy

- **Sono previste sanzioni amministrative fino a 20 milioni di Euro;**
- **È prevista la responsabilità civile nei confronti dell'interessato che subisca un danno materiale o immateriale causato da una violazione del GDPR;**
- **Le sanzioni penali possono essere previste dal Legislatore nazionale.**

SANZIONI AMMINISTRATIVE

Fino a 10 milioni di euro (o al 2% del fatturato globale dell'anno precedente), in caso di violazione delle disposizioni in materia di:

- Obblighi del Titolare del trattamento e del Responsabile del trattamento;
- Obblighi dell'organismo di certificazione;
- Obblighi dell'organismo di controllo.

Fino a 20 milioni di euro (o al 4% del fatturato globale dell'anno precedente), in caso di violazione delle disposizioni in materia di:

- Principi di base del trattamento, comprese le condizioni relative al consenso;
- Diritti degli interessati;
- trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale;
- 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..

PROFILI RISARCITORI

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

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.

Il Titolare del trattamento o il Responsabile del trattamento è esonerato dalla responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile

ANTICORRUZIONE, TRASPARENZA E PROTEZIONE DEI DATI PERSONALI

LEGGE N. 241/1990

LEGGE N. 190/2012

DECRETO LEGISLATIVO N. 33/2013

DECRETO LEGISLATIVO N. 97/2016

LEGGE 6 NOVEMBRE 2012, N. 190

"Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella Pubblica Amministrazione"

OBIETTIVO: Il contrasto della corruzione e della cattiva amministrazione

«MALADMINISTRATION»

[…]
Atti e comportamenti che, anche se non consistenti in specifici reati, contrastano con la necessaria cura dell'interesse pubblico e pregiudicano l'affidamento dei cittadini nell'imparzialità delle amministrazioni e dei soggetti che svolgono attività di pubblico interesse.

LA TRASPARENZA È ELETTA A PRINCIPALE MISURA DI PREVENZIONE

COME GARANTIRE LA TRASPARENZA?

Attraverso l'acquisizione di informazioni pubbliche

STRUMENTI «CIVICI» DI ACQUISIZIONE DELL'INFORMAZIONE PUBBLICA

L. 241/1990
D. Lgs. 33/2013
D. Lgs. 97/2016

(ART. 1)

PRIMA	ADESSO
La trasparenza è intesa come accessibilità totale delle informazioni concernenti l'organizzazione e l'attività delle pubbliche amministrazioni, allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche	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

(ART. 2)

PRIMA	ADESSO
Le disposizioni del presente Decreto individuano gli obblighi di trasparenza concernenti l'organizzazione e l'attività delle Pubbliche Amministrazioni e le modalità per la sua realizzazione.	Le disposizioni del presente Decreto disciplinano **la libertà di accesso di chiunque ai dati e ai documenti detenuti dalle pubbliche amministrazioni e dagli altri soggetti di cui all'articolo 2-bis,** garantita, nel rispetto dei limiti relativi alla tutela di interessi pubblici e privati giuridicamente rilevanti, tramite l'accesso civico e tramite la pubblicazione di documenti, informazioni e dati concernenti l'organizzazione e l'attività delle pubbliche amministrazioni e le modalità per la loro realizzazione

(ART. 3)

PRIMA	ADESSO
Tutti i documenti, le informazioni e i dati oggetto di pubblicazione obbligatoria ai sensi della normativa vigente sono pubblici e chiunque ha diritto di conoscerli, di fruirne gratuitamente, e di utilizzarli e riutilizzarli ai sensi dell'articolo 7	Tutti i documenti, le informazioni e i dati **oggetto di accesso civico**, ivi compresi quelli oggetto di pubblicazione obbligatoria ai sensi della normativa vigente sono pubblici e chiunque ha diritto di conoscerli, di fruirne gratuitamente, e di utilizzarli e riutilizzarli ai sensi dell'articolo 7.

(ART. 5 – Accesso civico)

PRIMA	ADESSO
1. L'obbligo previsto dalla normativa vigente in capo alle pubbliche amministrazioni di pubblicare documenti, informazioni o dati comporta il diritto di chiunque di richiedere i medesimi, nei casi in cui sia stata omessa la loro pubblicazione.	1. Idem 2. Allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico, chiunque ha diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del presente decreto, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'articolo 5-bis.

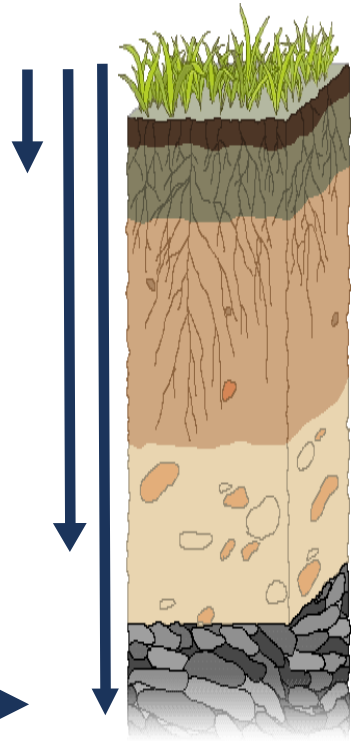
PATRIMONIO INFORMATIVO PUBBLICO

Accesso civico semplice: dati comuni e personali a pubblicazione obbligatoria non ancora pubblicati

Accesso civico generalizzato «FOIA» (Riservatezza>Accesso)
Dati comuni + alcuni dati personali

Accesso documentale 241/90 (Accesso>Riservatezza)
- Dati comuni + dati personali comuni
- Dati c.d. «sensibili e giudiziari»

ESCLUSIONI TASSATIVE
Ex art. 24 della L. 241/90



OBBLIGHI DI PUBBLICAZIONE

Accesso civico semplice, generalizzato e Accesso documentale

COS'È L'ACCESSO CIVICO: È un diritto introdotto dal D.Lgs. 33/2013 e ss.mm.ii.
Si distingue in:
- Accesso civico semplice che consente a chiunque - senza indicare motivazioni - il diritto di richiedere ad una Pubblica Amministrazione documenti, informazioni e dati nei casi in cui sia stata omessa la loro pubblicazione;
- Accesso civico generalizzato che consente a chiunque - senza indicare motivazioni - il diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti.

COS'È L'ACCESSO DOCUMENTALE: È il tradizionale accesso agli atti, previsto dall'art.22 della Legge n.241/1990, che permette a chiunque di richiedere documenti, dati e informazioni detenuti da una Pubblica Amministrazione riguardanti attività di pubblico interesse, purché il soggetto che lo richiede abbia un interesse diretto, concreto e attuale rispetto al documento stesso.

DIRITTI A CONFRONTO

	Accesso 241/90	Accesso FOIA D.Lgs. n. 33/2013
SOGGETTI	I soggetti privati, compresi quelli portatori di interessi pubblici o diffusi, che abbiano un **interesse diretto, concreto e attuale**, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso	**Chiunque**, senza necessità di motivazione

	Accesso 241/90	Accesso FOIA D.Lgs. n. 33/2013
OGGETTI	**Documenti amministrativi** [accesso si estende a documenti connessi. Non sono accessibili: le informazioni che non abbiano forma di documento amministrativo; i documenti amministrativi che la PA non ha (più) l'obbligo di detenere. La PA non è tenuta ad elaborare dati in suo possesso al fine di soddisfare le richieste di accesso].	**Dati, informazioni e documenti** detenuti

	Accesso 241/90	Accesso FOIA D.Lgs. n. 33/2013
FINALITÀ	Non sono ammissibili istanze di accesso preordinate ad un controllo generalizzato dell'operato delle Pubbliche Amministrazioni.	Favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e promuovere la partecipazione al dibattito pubblico.

	Accesso 241/90	Accesso FOIA D.Lgs. n. 33/2013
ESCLUSIONI	**Art 24:** Documenti coperti da segreto di Stato; altri casi di segreto (industriale, d'ufficio, ecc) o divieto di divulgazione espressamente previsti dalla legge; nei procedimenti tributari (in cui si applica la normativa speciale); attività diretta all'emanazione di atti normativi, amministrativi generali, di pianificazione e di programmazione; nei procedimenti selettivi, i documenti contenenti informazioni di carattere psicoattitudinale relativi a terzi. **MA** accesso parziale e differimento **MA** l'accesso prevale se necessario per curare o per difendere i propri interessi giuridici. Nel caso di documenti contenenti dati sensibili e giudiziari, l'accesso è consentito nei limiti in cui sia strettamente indispensabile e nei termini previsti dall'art. 60 del Codice Privacy in caso di dati idonei a rivelare lo stato di salute e la vita sessuale	Nei casi in cui sia necessario evitare un pregiudizio concreto a: Interessi pubblici, La sicurezza pubblica e l'ordine pubblico, La sicurezza nazionale, La difesa e le questioni militari, Le relazioni internazionali, La politica e la stabilità finanziaria ed economica dello Stato, La conduzione di indagini sui reati e il loro perseguimento, Il regolare svolgimento di attività ispettive. Interessi privati La protezione dei dati personali, in conformità con la disciplina legislativa in materia; La libertà e la segretezza della corrispondenza; Gli interessi economici e commerciali di una persona fisica o giuridica, ivi compresi la proprietà intellettuale, il diritto d'autore e i segreti commerciali. Segreto di Stato e altri casi di divieti di accesso o divulgazione previsti dalla legge, **MA** accesso parziale e differimento

	Accesso 241/90	Accesso FOIA D.Lgs. n. 33/2013
CONTRO-INTERESSATI	I soggetti, individuati o facilmente individuabili in base alla natura del documento richiesto, che dall'esercizio dell'accesso vedrebbero compromesso il loro diritto alla riservatezza	I soggetti che potrebbero subire un pregiudizio concreto alla tutela degli interessi privati

	Accesso 241/90	Accesso FOIA D.Lgs. n. 33/2013
TERMINI E SILENZIO	Decorsi inutilmente trenta giorni dalla richiesta, questa si intende respinta [«silenzio significativo»: SILENZIO ≡ RIGETTO]	Il procedimento di accesso civico deve concludersi con provvedimento espresso e motivato nel termine di trenta giorni dalla presentazione dell'istanza [SILENZIO = INADEMPIMENTO]

	Accesso 241/90	Accesso FOIA D.Lgs. n. 33/2013
COSTI	Il rilascio di copia è subordinato al rimborso del costo di riproduzione, salve le disposizioni vigenti in materia di bollo, nonché i diritti di ricerca e di visura	Il rilascio di dati o documenti in formato elettronico o cartaceo è gratuito, salvo il rimborso del costo effettivamente sostenuto e documentato dall'amministrazione per la riproduzione su supporti materiali

	Accesso 241/90	Accesso FOIA D.Lgs. n. 33/2013
TUTELA	Ricorso a Difensore civico/Commissione per l'accesso ai documenti amministrativi Ricorso al TAR	Istanza di riesame a RPC/Difensore civico Ricorso al TAR

I «TRE ACCESSI» A CONFRONTO
Esempio: Selezione pubblica

	Ho un interesse specifico (sono un partecipante)	Non ho trovato online documenti e/o informazioni che la PA è obbligata a pubblicare	Ho un interesse generico ad acquisire documenti e/o informazioni sulla procedura
STRUMENTI	**Accesso L. 241/1990**	**Accesso civico «semplice»**	**Accesso civico «generalizzato»**
COSA POSSO OTTENERE	Tutti gli atti della procedura (ivi compresi quelli contenenti dati sensibili, giudiziari e salute riferiti ai candidati – con opportuni accorgimenti)	I bandi di concorso (i singoli bandi e l'elenco di quelli espletati); i criteri di valutazione della Commissione; le tracce delle prove scritte	Tutto ciò il cui accesso non arrechi un pregiudizio concreto alla tutela dei dati personali del terzo. Esempio: le graduatorie concorsuali, una volta che siano rimosse dall'albo online; le prove scritte svolte dai candidati; ecc…

RESPONSABILITÀ E SANZIONI

- **Da 1.000 a 10.000 euro (artt. 24-quater, c.1 e 19, c.5., lett. b, d.l. 90/14)**
- **Da 1.000 a 10.000 euro (artt. 24-quater, c.1 e 19, c.5., lett. b, d.l. 90/14)**

• omessa adozione dei PTPC e dei codici di comportamento;

- **Controllo regolare attuazione dell'accesso civico:**

• Inadempimento di obblighi pubblicazione previsti dalla normativa vigente e il rifiuto, il differimento e la limitazione dell'accesso civico, al di fuori delle ipotesi previste dall'articolo 5-bis.

- **«Troppa» trasparenza o «troppo poca»:**

• Pubblicazione eccessiva. L'amministrazione può essere tenuta al risarcimento del danno per trattamento illecito dei dati personali da parte di un suo dipendente. Rivalsa nei confronti del dipendente soggetta alla dimostrazione di dolo/colpa grave.
• Pubblicazione eccessiva. L'amministrazione è sanzionata dal Garante privacy. Rivalsa nei confronti del dipendente in caso di dolo/colpa grave.
• Inadempimento doveri di trasparenza.

TRASPARENZA O PRIVACY

Dove un superiore pubblico interesse non imponga un momentaneo segreto, la casa dell'amministrazione dovrebbe essere di vetro

Ma i suoi abitanti devono comunque rimanere vestiti

PUBBLICI
(esigenza di conoscibilità - ampliamento delle occasioni di uso/riuso)

A CARATTERE PERSONALE
(esigenza di protezione - limitazione e controllo di uso/riuso)

CENNI

- ILLECITO diffondere (es. pubblicare online) dati personali in assenza di una norma di legge/regolamento che lo prescriva;
- Nei casi in cui norme di legge o di regolamento prevedano la pubblicazione di atti o documenti, le Pubbliche Amministrazioni provvedono a rendere NON INTELLIGIBILI i dati personali non pertinenti o, se c.d. «sensibili o giudiziari», non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione,
- Importanza dell'uso della FIRMA DIGITALE per evitare il proliferare online di firme autografe

PROBLEMATICHE

- Pubblicazione di graduatorie (sia definitive che intermedie) - Pubblicazione di graduatorie di beneficiari di sussidi per disagio economico con indicazione di dati personali o di iniziali del nome/cognome e con possibilità di risalire all'identità dei beneficiari incrociando le informazioni con altre facilmente reperibili sul web [IN ENTRAMBE LE IPOTESI NON SI TRATTA DI ANONIMIZZAZIONE] - [**IL GARANTE PRIVACY HA SANZIONATO CASI SIMILI**]
- Persistenza di curriculum con dati eccedenti o pubblicazione di atti non richiesti contenenti dati personali

GRAZIE DELL'ATTENZIONE

Dott. Pasquale Nicolazzo

Data Protection Officer

info@studionicolazzo.it

www.studionicolazzo.it