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

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 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.

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,

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

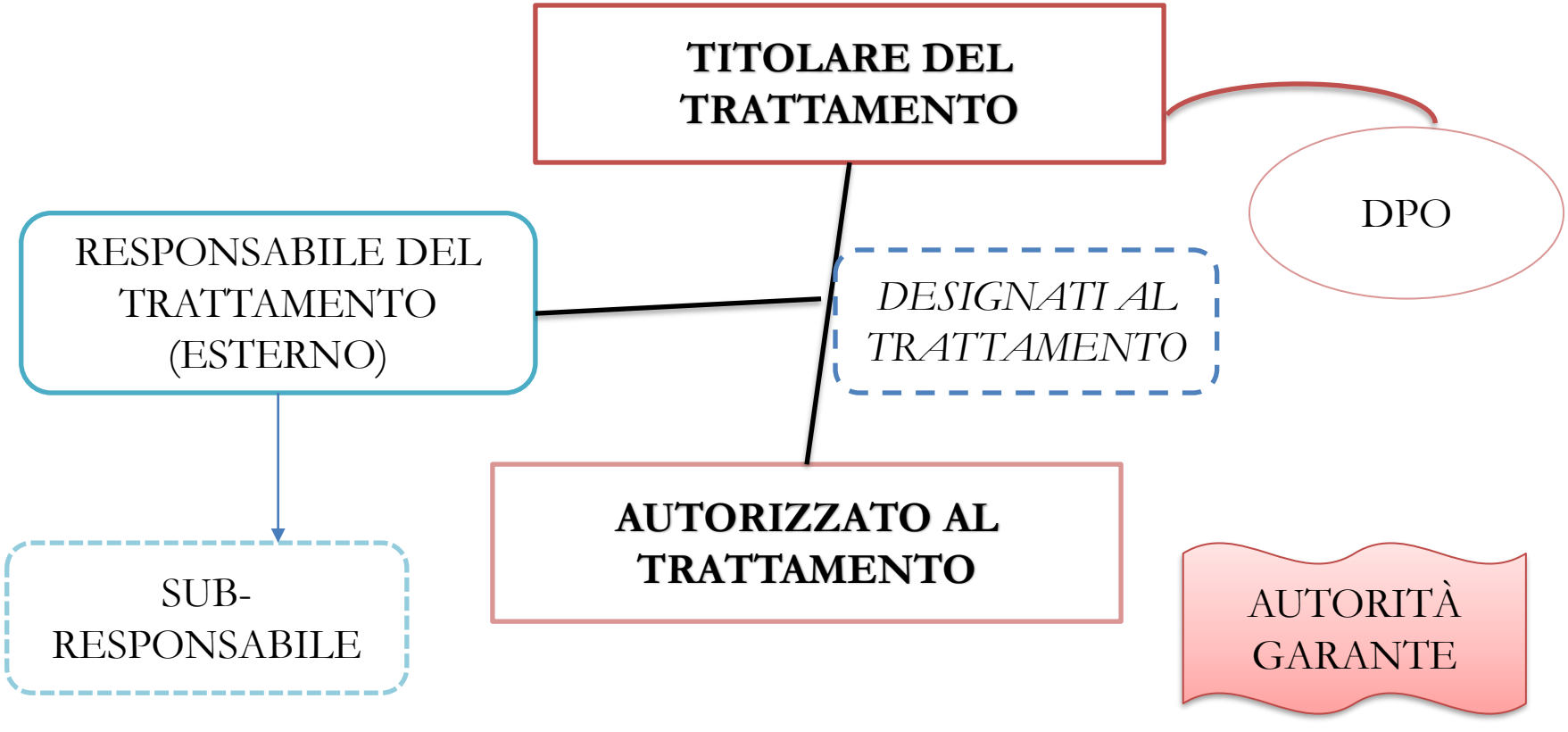
Dalla forma alla sostanza

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.

I RUOLI PREVISTI DAL GDPR



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

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)

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

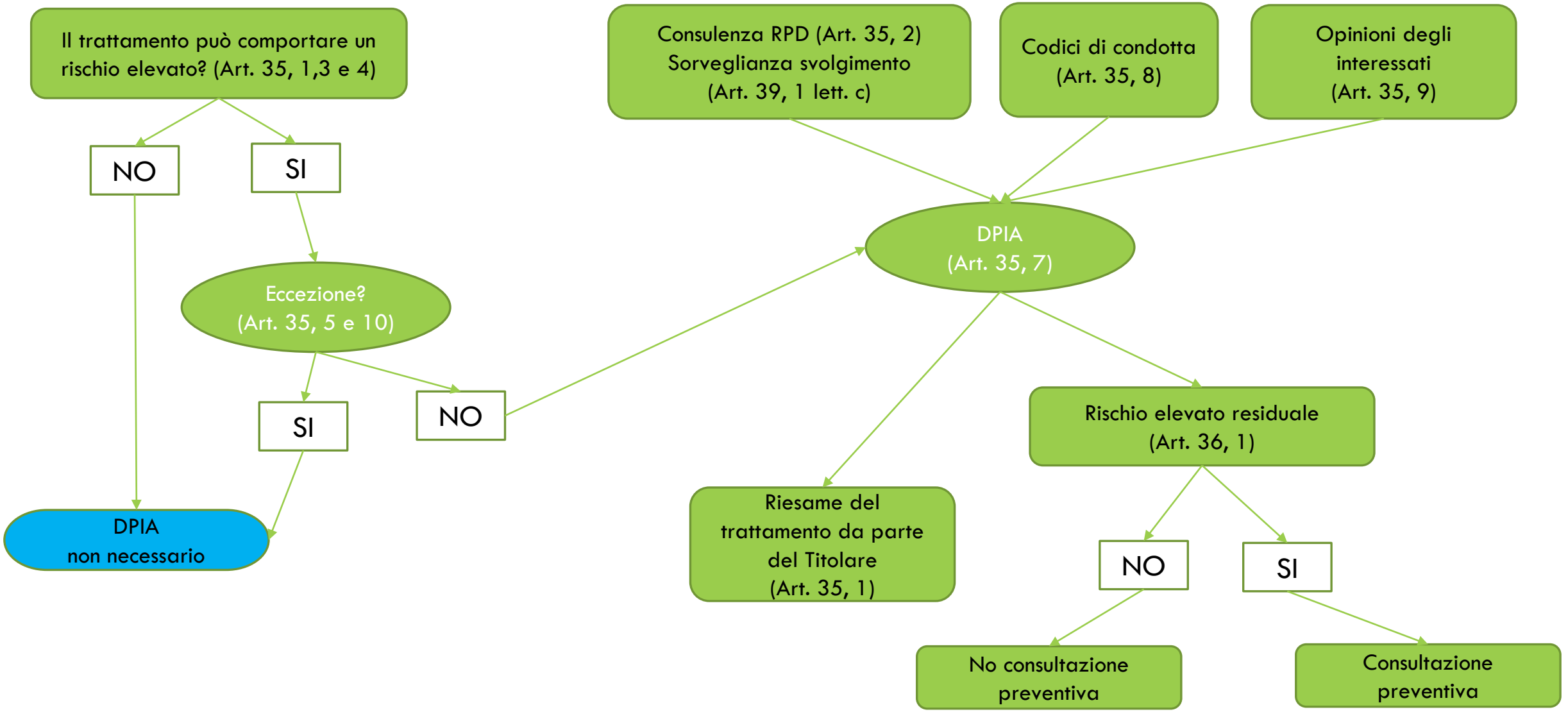
In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione 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

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

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI – QUANDO EFFETTUARLA ?



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..

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

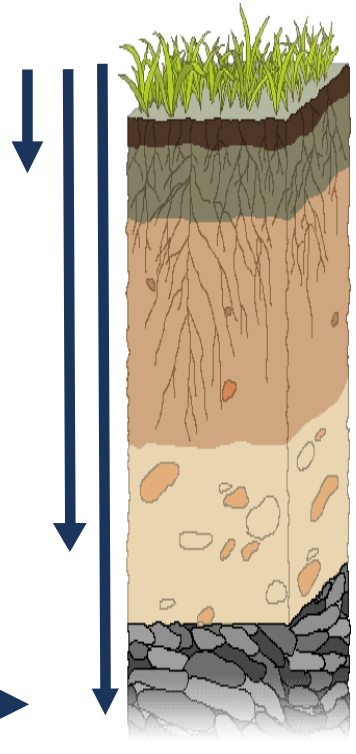
PATRIMONIO INFORMATIVO PUBBLICO

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.

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)

GRAZIE DELL'ATTENZIONE

Dott. Pasquale Nicolazzo

Data Protection Officer

info@studionicolazzo.it

www.studionicolazzo.it