FSE 2014-2020 POR BasilicataEuropa

REGIONE BASILICATA

Unione Europea
Fondo Sociale Europeo

Regolamento Generale sulla Protezione dei Dati

Nicola Petrizzi – DPO Regione Basilicata

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

REGIONE BASILICATA

REGOLAMENTO (UE) 2016/679
DEL PARLAMENTO EUROPEO E DEL CONSIGLIO
DEL 27 APRILE 2016
RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI, NONCHÉ ALLA LIBERA CIRCOLAZIONE DI TALI DATI E CHE ABROGA LA DIRETTIVA 95/46/CE

GDPR

***R**egolamento **G**enerale sulla **P**rotezione dei **D**ati*

Quante persone tratteranno i DATI personali ?

250 Nuclei familiari

1.000 persone

- Regione Basilicata
- 22 Beneficiari Capofila
- 44 Partner
- 56 Comuni Destinatari delle Attività
- 9 Comuni Capofila
- 2 Aziende Sanitarie

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

IL NUOVO SCENARIO DIGITALE MOSTRA CHE LA RETE È PERVASIVA, IMMATERIALE ED IMMEDIATAMENTE DISPONIBILE A MOLTI UTENTI

LA RAPIDITÀ E L'INTENSITÀ
DELL'EVOLUZIONE TECNOLOGICA
HANNO CONDOTTO ALL'AUMENTO DI
SOGGETTI ED OGGETTI CONNESSI FRA
LORO (PER QUESTO SI PARLA DI RETE DELLE
COSE, **INTERNET OF THINGS, IOT**).

SI ASSISTE AL CONSEGUENTE
SCAMBIO E CONDIVISIONE DI DATI FRA
INDIVIDUI ED ORGANIZZAZIONI
DI DIVERSO GENERE E TIPO
(O SCOPO, QUALI ISTITUZIONI, IMPRESE, ENTI
NO PROFIT, ETC.) IN TUTTO IL MONDO
SIA FISICO CHE DIGITALE.

Come oramai molti sanno il 25 maggio 2018 è entrato in vigore a livello di Comunità Europea il nuovo Regolamento Europeo sul trattamento dei dati personali.

- È un unico testo per tutti gli Stati membri dell'UE. L'obiettivo della Commissione Europea è quello di **semplificare il contesto normativo** che riguarda gli affari internazionali, garantendo a tutti i cittadini europei il controllo sui propri dati personali.
- Rimane solo un potere legislativo limitato agli Stati nazionali
- Abroga la direttiva europea 95/46/CE (era il principale strumento giuridico dell'Unione europea in materia di protezione dei dati)
- **Non abroga il D.Lgs. n.196 del 2003 "Codice della Privacy"** >
- Non abroga i provvedimenti del Garante

OGGETTO E FINALITA'

- La protezione delle persone fisiche con riguardo al Trattamento dei dati di carattere personale è **un diritto fondamentale.** L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha **diritto alla protezione dei dati di carattere personale** che la riguardano.

- 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.

- Esso **protegge i diritti e le libertà fondamentali delle persone fisiche,** in particolare il diritto alla protezione dei dati personali.

- La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al Trattamento dei dati personali.

- **Si applica alle persone fisiche**, a prescindere dalla nazionalità o dal luogo di residenza, in relazione al Trattamento dei loro dati personali. Quindi il presente regolamento **non disciplina** il Trattamento dei dati personali relativi a persone giuridiche, in particolare imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto.

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

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.**

Il GDPR esplicita i **TERMINI UTILIZZATI** offrendo una serie di **DEFINIZIONI** appositamente riportate all'interno dell'Articolo 4 ed opportunamente commentate con i rispettivi Considerando

1) «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;**

2) «trattamento»

qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come:

- la raccolta,
- la registrazione,
- l'organizzazione,
- la strutturazione,
- la conservazione,
- l'adattamento o la modifica,
- l'estrazione,
- la consultazione,
- l'uso,
- la comunicazione mediante trasmissione,
- diffusione o qualsiasi altra forma di messa a disposizione,
- il raffronto o l'interconnessione,
- la limitazione,
- la cancellazione o la distruzione;

4) «profilazione»

qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o
prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

5) «pseudonimizzazione»

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

6) «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;

7) «Titolare del trattamento»

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;

8) «Responsabile del trattamento»

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

9) «destinatario»

la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi.

10) «terzo»

la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia:

- l'interessato,
- il Titolare del trattamento,
- il Responsabile del trattamento,
- le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile;

in via residuale chiunque non possa essere annoverato nelle categorie soggettive previste dal Regolamento

11) «consenso dell'interessato»

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;

12) «violazione dei dati personali»

la violazione di 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;

Articolo 5 - Principi applicabili al trattamento di dati personali

1. I dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («**liceità, correttezza e trasparenza**»);

b) 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, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («**limitazione della finalità**»);

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («**minimizzazione dei dati**»);

d) 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**»);

e) 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; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («**limitazione della conservazione**»);

f) 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**»).

2. Il Titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («**responsabilizzazione**»).

Articolo 6 – Liceità del trattamento

1. 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 particolare se l'interessato è un minore.

La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

Articolo 6 – Liceità del trattamento

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, ovvero:

il **CONSENSO**
- l'adempimento ad **OBBLIGHI CONTRATTUALI**
- gli **INTERESSI VITALI** della persona interessata o di terzi
- gli **OBBLIGHI DI LEGGE** cui è soggetto il Titolare
- l'**INTERESSE PUBBLICO** o l'**ESERCIZIO DI PUBBLICI POTERI**
- l'**INTERESSE LEGITTIMO** prevalente del Titolare o di terzi cui i dati vengono comunicati.

4. Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il Titolare del trattamento tiene conto, tra l'altro:

   a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;
   b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il Titolare del trattamento;
   c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi condanne penali e a reati ai sensi dell'articolo 10;
   d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;
   e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

Articolo 7 Condizioni per il consenso

Qualora il trattamento sia basato sul consenso, il Titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.

2. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.

3. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.

4. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

Articolo 8 Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione

1. Qualora si applichi l'articolo 6, paragrafo 1, lettera a), per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore **abbia almeno16 anni.** Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal Titolare della responsabilità genitoriale.
   Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni.

L'Italia si è avvalsa della facoltà di stabilire un età inferiore a quella prevista "by default" dal GDPR. Il comma 1 dell'art. 2-quinquies del novellato Codice Privacy ed introdotto dal D.Lgs. 101/2018 dispone: In attuazione dell'articolo 8, paragrafo 1, del Regolamento, ***il minore che ha compiuto i quattordici anni può esprimere il consenso*** *al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione. Con riguardo a tali servizi, il trattamento dei dati personali del minore di età inferiore a quattordici anni, fondato sull'articolo 6, paragrafo 1, lettera a), del Regolamento, è lecito a condizione che sia prestato da chi esercita la responsabilità genitoriale.*

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.

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)

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)

- Il riscontro all'interessato deve essere in **forma scritta** anche attraverso strumenti elettronici che ne favoriscano l'accessibilità; può essere dato **oralmente solo se richiesto dall'interessato** (art. 12, paragrafo 1; e art. 15, paragrafo 3).

- La risposta fornita all'interessato deve essere "intelligibile", concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.

L'informativa all'interessato

Il GDPR (art.13) **amplia i contenuti dell'informativa** che deve essere fornita, da parte del Titolare del trattamento, all'interessato a tutela dell'esercizio della protezione dei dati.

Cosa cambia?

- ✓ **i dati di contatto del Responsabile della protezione dei dati** (DPO)
- ✓ la descrizione delle finalità perseguite
- ✓ **la base giuridica del trattamento** (norma, contratto, ecc.)
- ✓ gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali
- ✓ l'intenzione del Titolare del trattamento di trasferire i dati all'estero
- ✓ le modalità del trattamento (soprattutto se automatizzate)
- ✓ **il periodo di conservazione dei dati o i criteri** seguiti **per stabilire tale periodo**
- ✓ **il diritto dell'interessato di ottenere la limitazione del trattamento**
- ✓ **Il diritto alla portabilità dei dati**
- ✓ **Il diritto di presentare un reclamo all'autorità di controllo**

I soggetti pubblici non devono, di regola, chiedere il consenso per il Trattamento dei dati personali

(su questo punto valgono il considerando 43, art. 9 del GDPR altre disposizioni del Codice Privacy).

CONTENUTI DELL'INFORMATIVA

I contenuti dell'informativa sono elencati **in modo tassativo** dal Regolamento negli articoli 13, paragrafo 1, e 14, paragrafo 1, del regolamento e in parte **SONO PIÙ AMPI RISPETTO AL CODICE**. In questo senso il Regolamento prevede che **IL Titolare DEVE SEMPRE** specificare:

- i **dati di contatto del Responsabile per la Protezione dei Dati (in italiano RPD oppure in inglese DPO) se** esistente
- la **base giuridica** del Trattamento
- **qual è il suo interesse legittimo** se quest'ultimo costituisce la base giuridica del Trattamento.

CONTENUTI DELL'INFORMATIVA

Inoltre il Titolare **DEVE SEMPRE** specificare

se trasferisce i dati personali in Paesi terzi e, in caso affermativo, **attraverso quali strumenti,** come ad esempio:

si tratta di un Paese terzo giudicato adeguato dalla Commissione europea si utilizzano Regole Vincolanti per aziende multinazionali con più sedi locali (Binding Corporate Rules – BCR) per trasferimenti infragruppo sono state inserite specifiche clausole contrattuali modello, ecc..

CONTENUTI DELL'INFORMATIVA

Il Regolamento prevede anche ulteriori informazioni in quanto «necessarie per garantire un Trattamento corretto e trasparente». In particolare, il Titolare deve specificare:

- il **periodo di conservazione dei dati** o i criteri seguiti per stabilire tale periodo di conservazione;
- il diritto di presentare un reclamo all'autorità di controllo
- se il Trattamento comporta processi decisionali automatizzati (anche la profilazione), l'informativa deve specificarlo
- deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l'Interessato.

TEMPI DELL'INFORMATIVA

Nel caso di dati personali **non raccolti direttamente presso l'Interessato** l'informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta,

oppure al momento della comunicazione (NON della registrazione) dei dati (a terzi o all'Interessato)

MODALITÀ DELL'INFORMATIVA

Il Regolamento specifica molto più in dettaglio rispetto al Codice le caratteristiche dell'informativa, che deve avere forma

concisa
trasparente
intelligibile
e facilmente accessibile per l'Interessato

occorre utilizzare un linguaggio **chiaro e semplice,** e per i minori occorre prevedere informative idonee (come riportato anche dal Considerando 58).

MODALITÀ DELL'INFORMATIVA

L'informativa è **data, in linea di principio, per iscritto** e **preferibilmente in formato elettronico** (soprattutto nel contesto di servizi online) anche se sono **ammessi "altri mezzi"**, quindi può essere fornita **anche oralmente,** ma nel rispetto delle caratteristiche di cui sopra (art. 12, paragrafo 1).

Il Regolamento ammette l'utilizzo di **icone** per presentare i contenuti dell'informativa in forma sintetica, **ma solo "in combinazione" con l'informativa estesa.** Le icone dovranno essere identiche in tutta l'Ue e saranno definite prossimamente dalla Commissione europea.

MODALITÀ DELL'INFORMATIVA

L'informativa deve essere fornita all'Interessato **prima di effettuare la raccolta dei dati** (se raccolti direttamente presso l'Interessato, come si evince nell'art. 13).

Se i dati non sono raccolti direttamente presso l'Interessato (art.14), l'informativa deve comprendere anche le **categorie** dei dati personali oggetto di Trattamento.

MODALITÀ DELL'INFORMATIVA

In tutti i casi, il Titolare deve specificare **la propria identità e quella dell'eventuale rappresentante nel territorio italiano,** le **finalità del Trattamento,** i **diritti degli interessati** (compreso il diritto alla portabilità dei dati), se esiste un **Responsabile del Trattamento e la sua identità, e quali sono i destinatari dei dati.**

NOTA: ogni volta che le finalità cambiano si impone di informarne l'Interessato prima di procedere al Trattamento ulteriore.

Articolo 14 - **Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato**

1. Qualora i dati non siano stati ottenuti presso l'interessato, il Titolare del trattamento fornisce all'interessato le seguenti informazioni:
   a) l'identità e i **dati di contatto del Titolare del trattamento** e, ove applicabile, del suo rappresentante;
   b) i dati di **contatto del Responsabile della protezione dei dati,** ove applicabile;
   c) le **finalità del trattamento** cui sono destinati i dati personali nonché la base giuridica del trattamento;
   d) le categorie di dati personali in questione;
   e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
   f) ove applicabile, l'intenzione del Titolare del trattamento di **trasferire dati** personali a un destinatario in un paese terzo o a un'organizzazione internazionale ….;

2. Oltre alle informazioni di cui al paragrafo 1, il Titolare del trattamento fornisce all'interessato le seguenti informazioni necessarie per garantire un trattamento corretto e trasparente nei confronti dell'interessato:
   a) il **periodo di conservazione** dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
   b) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal Titolare del trattamento o da terzi;
   c) l'esistenza del **diritto dell'interessato** di chiedere al Titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
   d) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca;
   e) il **diritto di proporre reclamo** a un'autorità di controllo;
   f) la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;
   g) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

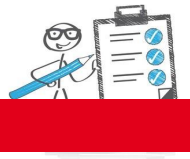
Articolo 14 - **Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato** GDPR

3.Il Titolare del trattamento fornisce le informazioni di cui ai paragrafi 1 e 2:

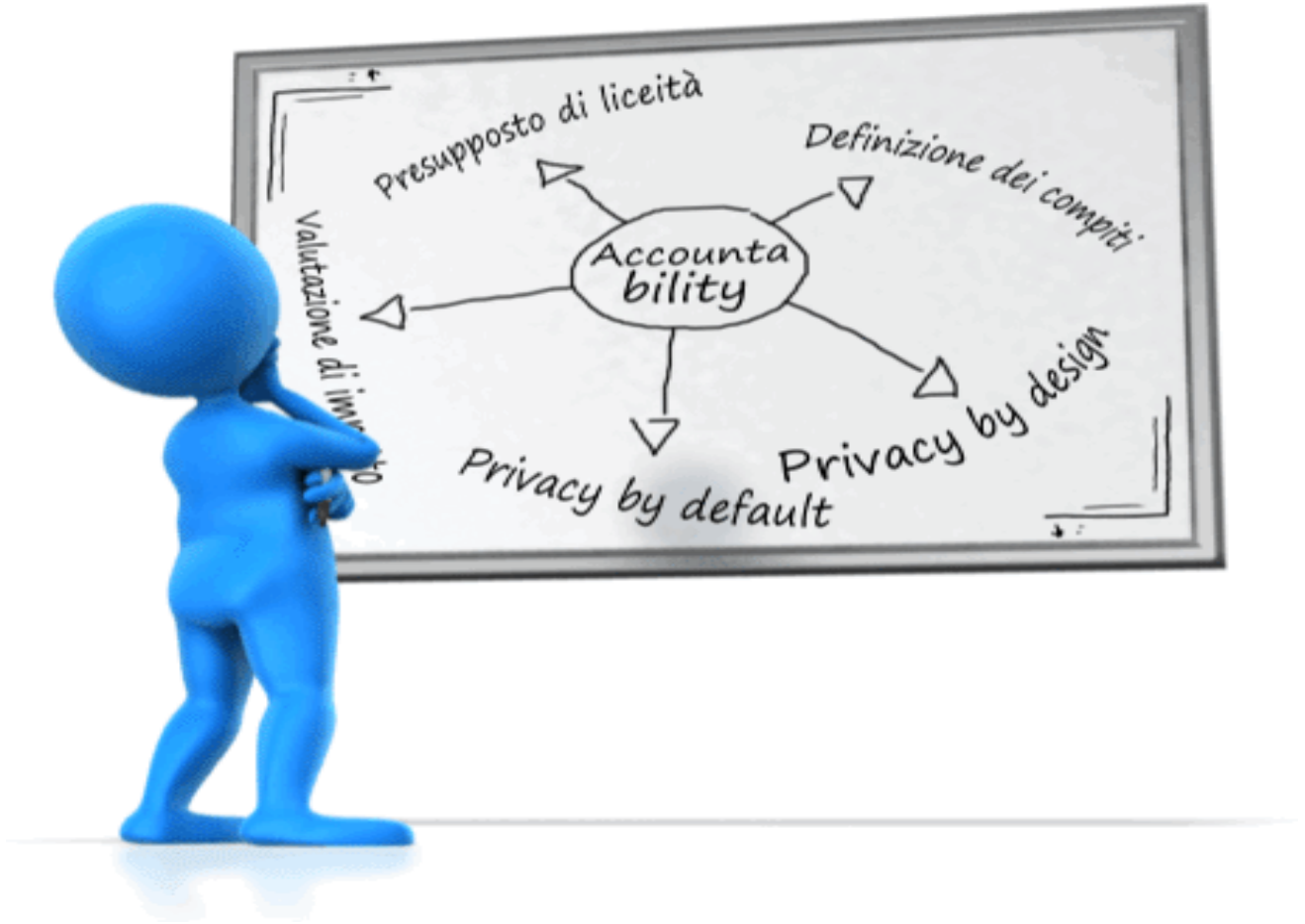
a) entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;
b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; oppure
c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.

4.Qualora il Titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati ottenuti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni informazione pertinente di cui al paragrafo 2. 5.I paragrafi da 1 a 4 non si applicano se e nella misura in cui:

a) l'interessato dispone già delle informazioni;
b) comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1, o nella misura in cui l'obbligo di cui al paragrafo 1 del presente articolo rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In tali casi, il Titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni;
c) ……..



Necessità di un approccio sistemico



Dalla forma alla sostanza

L’accountability e l’approccio basato sul rischio Considerando 74 (art. 5, par. 2 e art. 24)

Uno dei principi fondamentali sul quale si fonda il GDPR è senza dubbio il principio di Accountability.

Il termine in inglese utilizzato dal legislatore europeo per esprimere il concetto di cui si parla trova in italiano la traduzione più adatta in “responsabilizzazione”.

il termine “accountability” non è facilmente traducibile. Da un punto di vista lessicale il termine in questione è una parola composta. Il verbo **to account** è traducibile in italiano come **“dar conto”.** Il sostantivo “**ability**” significa “**essere in grado di**” o “**avere attitudine a**”.

Il concetto di “accountability” è legato al rendere conto dell’azione fatta o fatta fare (essere in grado di comprovarlo), al rispondere e al rendere conto dei risultati ottenuti, delle cose fatte (fatte bene e fatte male)

L’esigenza soddisfatta dall’introduzione del principio di responsabilizzazione è quella di far in modo che i soggetti che determinano finalità e mezzi del trattamento, o che trattano i dati per loro conto, dunque il **Titolare ed il Responsabile del trattamento, fossero spinti a porre in essere tutte le misure necessarie alla protezione effettiva del dato personale oggetto dei trattamenti.**

L’accountability e l’approccio basato sul rischio Considerando 74 (art. 5, par. 2 e art. 24)

Tenuto conto

della natura

dell’ambito di applicazione

del contesto

delle finalità del trattamento

dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche

Il Titolare del trattamento mette in atto misure

Tecniche

organizzative

adeguate

garantire

ed essere in grado di dimostrare

che il trattamento è effettuato conformemente al regolamento

L'accountability e l'approccio basato sul rischio Considerando 74 (art. 5, par. 2 e art. 24)

Sarà necessario **elaborare un sistema documentale di gestione della privacy** contenente tutti gli atti, regolarmente aggiornati, elaborati per soddisfare i requisiti di conformità al Regolamento.

Viene introdotto l'obbligo di **istituire un registro del trattamenti dei dati e** l'applicazione operativa del **principio di rendicontazione e responsabilità** (o di "**accountability**"), secondo cui il Titolare del trattamento deve conservare la documentazione di tutti i trattamenti effettuati sotto la propria responsabilità, indicando obbligatoriamente, per ognuno di essi, una serie "nutrita" di informazioni, tali da assicurare e comprovare la conformità di ciascuna operazione alle disposizioni del Regolamento (qualcosa di simile al Documento Programmatico sulla Sicurezza, ma di portata più ampia).

Tutte le operazioni di trattamento devono essere tracciabili e documentabili.

E' la logica della «SCATOLA NERA»

- Privacy by design e by default (art. 25)
- Sicurezza (art. 32)
- Data Breach (artt. 33-34)
- **Data Protection Impact Assessment - DPIA (artt. 35-36)**

Art. 25 - Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

L'entrata in vigore del nuovo Regolamento europeo in materia di protezione dei dati personali, di fatto, ha **modificato radicalmente l'approccio adottato finora per la regolamentazione della materia**, introducendo in modo espresso nel sistema legislativo di settore principi prima estranei al nostro ordinamento (si pensi, ad esempio, al concetto di **privacy by design e privacy by default**) ed attribuendo, tra questi, un ruolo di centralità a quello così detto di "responsabilizzazione" del Titolare e del Responsabile del trattamento.

Attraverso processi documentati (scelte fatte e motivazioni):
Privacy by design
In tutte le fasi del ciclo di vita del trattamento (sia cartaceo che informatico) – Progettazione, messa in esercizio, Utilizzo e dismissione finale.

Privacy by default
Tutela della protezione dei dati - Minimizzazione e Limitazione della finalità.

Art. 25 - Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

Il principio di «privacy by design» - o di «protezione dei dati personali fin dalla progettazione» -

prevede che ogni Titolare o Responsabile del trattamento debba tenere in considerazione, sin dalla ideazione e progettazione delle attività di trattamento che intende porre in essere, la protezione della riservatezza dei dati personali degli interessati cui il trattamento si riferisce.

Effettuare il trattamento nel rispetto della norma, minimizzando i rischi e rispettando la tutela degli interessati.

Il principio di «privacy by default» - o di «protezione dei dati personali «per impostazione predefinita»

prevede che ogni Titolare o Responsabile effettui il trattamento dei soli dati personali degli interessati nella misura e per il tempo necessari a raggiungere le specifiche finalità del trattamento, implementando, all'interno degli ambienti, dei sistemi informatici e delle infrastrutture di rete utilizzate per tale trattamento, le misure tecniche idonee a proteggere i dati personali degli interessati.

Trattare solo dati necessari per raggiungimento delle finalità del trattamento.

Art. 25 - Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

Il Primo paragrafo dell'art. 25 del GDPR

racchiude l'essenza del c.d. "risk based approach": il Titolare del trattamento deve progettare (ecco il "by design") ed effettuare il trattamento tenendo in considerazione i rischi per i diritti e le libertà dei soggetti interessati. **E' proprio tale valutazione iniziale che determina l'entità della responsabilità del Titolare e del Responsabile del trattamento,** tenuto della natura, del contesto e delle finalità del trattamento.

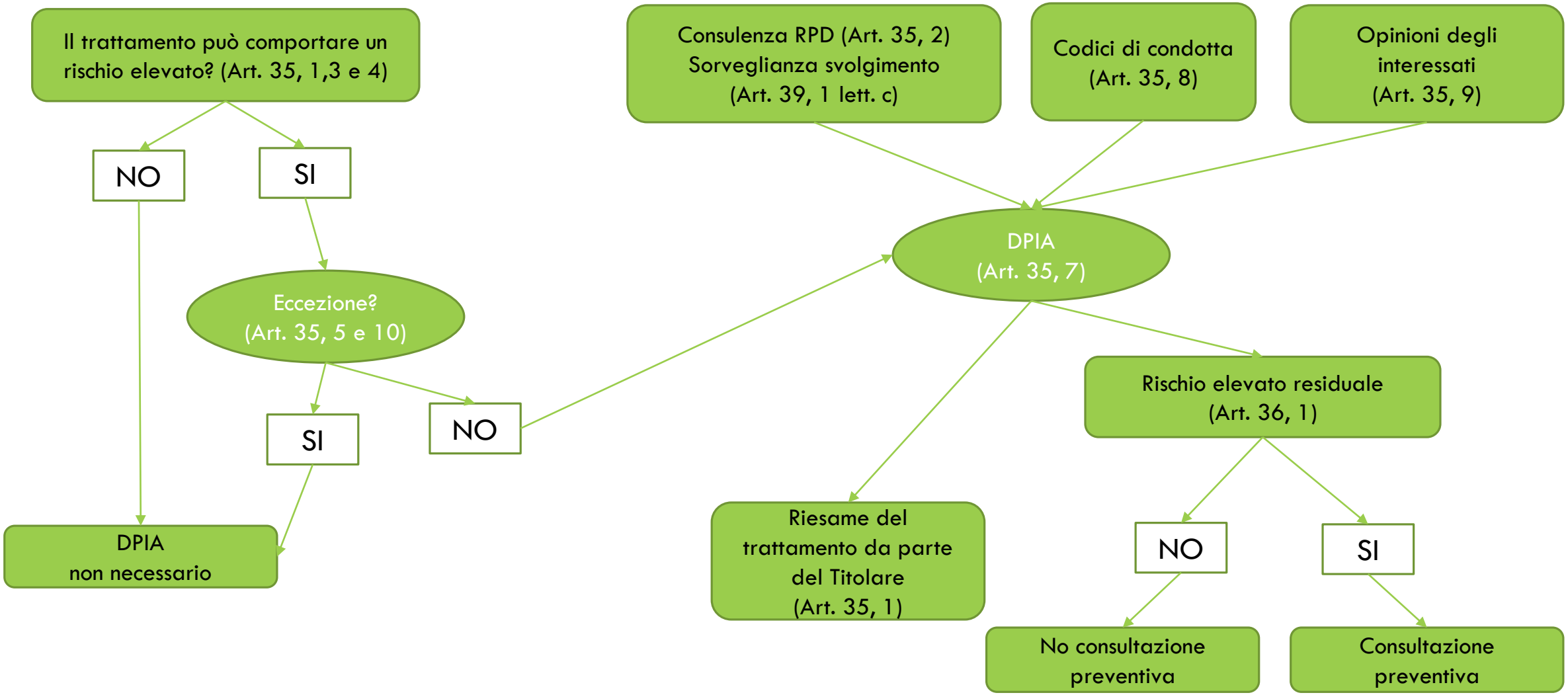
Il Considerando 78 esplicita le caratteristiche di alcune delle misure tecniche richieste "by design" al Titolare del trattamento
"Tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, pseudonimizzare i dati personali il più presto possibile, offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali, consentire all'interessato di controllare il trattamento dei dati e consentire al Titolare del trattamento di creare e migliorare caratteristiche di sicurezza. In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati"

Il Secondo Comma dell'art. 25 – Privacy by Default

Chi organizza il trattamento dei dati personali è tenuto ad implementare misure tecniche e organizzative (anche in questo caso si tratta di accorgimenti di natura informatica e gestionale) che garantiscano in ogni momento che il volume di dati trattati sia il più contenuto possibile, ossia che siano trattati esclusivamente i dati personali strettamente necessari per le finalità del trattamento. L'analisi e la definizione delle opportune misure necessarie ad assicurare costantemente la minimizzazione del trattamento dev'essere personalizzata rispetto a tale trattamento: vanno infatti considerati tutti gli aspetti necessari a renderlo "**minimo**", in particolare la qualità e quantità dei dati, l'estensione ed entità del complessivo trattamento, la durata del periodo di retention e il tipo di accessibilità prevista per i dati trattati. Elemento chiave, anche in tale ambito, sarà la corretta definizione e attuazione di policies che consentano di verificare e documentare che l'impostazione predefinita del trattamento è idonea a **ridurre il volume dei dati personali trattamenti al minimo necessario richiesto dalle finalità del trattamento.**

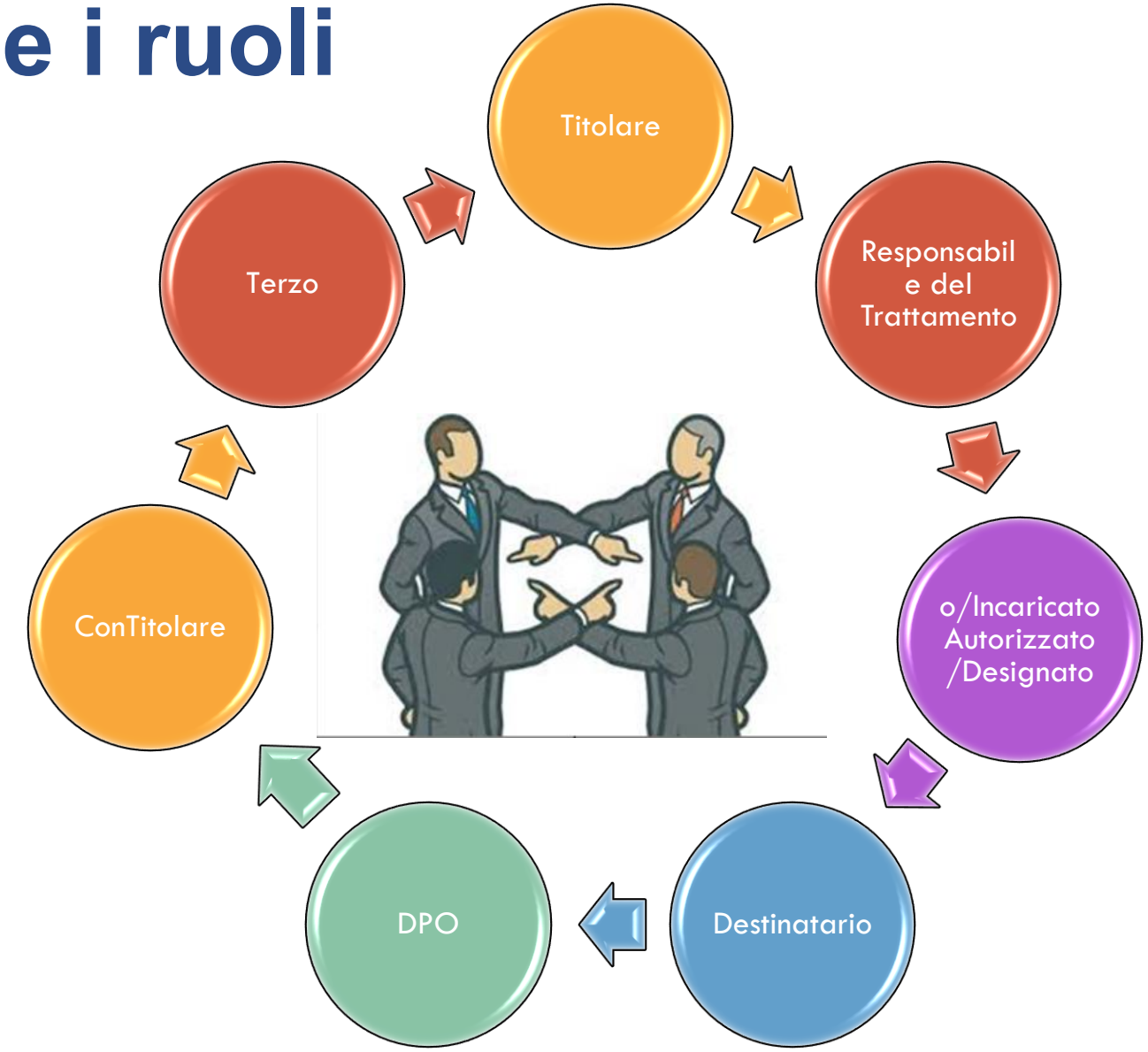
D.P.I.A. - *Data Protection Impact Assessment*

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI – QUANDO EFFETTUARLA ?



Gli attori principali

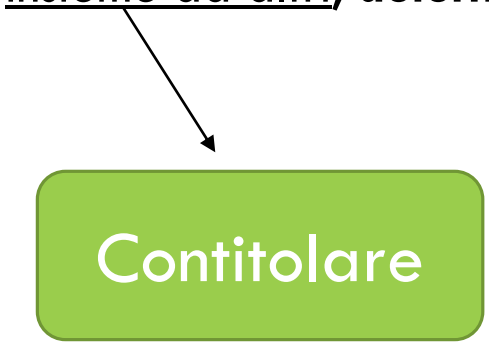
Gli attori e i ruoli



Titolare	Disciplina la contitolarità del trattamento (art. 26): «quando due o più titolari determinano congiuntamente le finalità e i mezzi del trattamento essi definiscono in un accordo interno le rispettive responsabilità in merito all'osservanza degli obblighi del GDPR Definisce (art. 4 .8) il Responsabile del trattamento come «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento»
Responsabile	Fissa, poi, più dettagliatamente (rispetto all'art. 29 del Codice) le caratteristiche dell'atto con cui il Titolare designa un Responsabile del trattamento attribuendogli specifici compiti (art. 28) Consente la nomina di sub-responsabili del trattamento da parte di un Responsabile (art. 28 com. 4), per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano Titolare e Responsabile primario
Autorizzati	Non prevede espressamente la figura dell'"incaricato" del trattamento (ex art. 30 del Codice), ma non ne esclude la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile" (art. 4 com. 10)

«Titolare del trattamento»

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.



«Responsabile del trattamento»

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

Il Responsabile può nominare sub-responsabili per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano Titolare e «Responsabile primario».

ATTENZIONE

Il «Responsabile primario» **risponde dinanzi al Titolare dell'inadempimento del sub-Responsabile**, anche ai fini del risarcimento di eventuali danni causati dal trattamento.

«Responsabile del trattamento»

Necessità di un **contratto o altro atto giuridico (art.28)** che vincoli il Responsabile al Titolare e che disciplini:

- Materia e durata del trattamento;
- Natura e finalità del trattamento;
- Tipo di dati personali e categorie di interessati;
- Obblighi e diritti del Titolare del trattamento.

In base al contratto **il Responsabile si impegna** a:

a. **Trattare dati** soltanto **su istruzione** documentata **del Titolare;**
b. **Consentire i trattamenti solo a persone autorizzate** con impegno alla riservatezza o che abbiano un adeguato obbligo legale di riservatezza;
c. **Adottare tutte le misure di sicurezza** (es. cifratura; pseudonimizzazione; recupero da backup);
d. Rispettare le condizioni per ricorrere a un sub-Responsabile del trattamento;
e. Assistere il Titolare per dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
f. **Cancellare o restituire tutti i dati** e cancellare le copie esistenti;
g. Mettere a disposizione del Titolare le informazioni per dimostrare il rispetto dei suddetti obblighi e **consentire le ispezioni.**

Le nuove figure

Alle consuete figure del Titolare, del Responsabile, dell'autorizzato/incaricato e dell'interessato il

Regolamento affianca:

1. **Il Responsabile della protezione dei dati**, meglio noto come «Data Protection Officer (DPO)».

2. **Il destinatario dei dati:** la persona fisica o giuridica (sia pubblica che privata) a cui vengono comunicati i dati personali.

3. **Il terzo**: in via residuale chiunque non possa essere annoverato nelle categorie soggettive previste dal Regolamento.

Principali compiti del Responsabile della Protezione Dati - DPO

Art.39

TRATTAMENTO SOTTO L'AUTORITÀ DEL TITOLARE DEL TRATTAMENTO O DEL RESPONSABILE DEL TRATTAMENTO (ART. 29)

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.

Esiste la figura dell’incaricato?

Pur non prevedendo espressamente la **figura dell' "incaricato" del trattamento** (ex art. 30 Codice PRIVACY), il regolamento **non ne esclude** la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile" *(si veda, in particolare, art. 4, n. 10, del regolamento)*.

«TERZO»

L'approccio del legislatore italiano

- Abrogazione delle disposizioni del previgente codice in **contrasto con il GDPR**;
- **Non duplicazione** di alcune disposizioni molto simili ma non coincidenti, presenti sia nel regolamento sia nel codice (es. le definizioni, l'informativa da rendere all'interessato ecc.)
- Mancato richiamo di alcune previsioni contenute nel previgente codice assorbite dalle norme del regolamento europeo;
- **Abrogazione delle misure minime di sicurezza** in coerenza con il principio di «*accountability*».

L'approccio del legislatore italiano

All'art. 22, comma 13 del D.lgs. 101/2018 si legge: "**Per i primi otto mesi dalla data di entrata in vigore del presente decreto,** il Garante per la protezione dei dati personali tiene conto, ai fini dell'applicazione delle sanzioni amministrative e nei limiti in cui risulti compatibile con le disposizioni del Regolamento (UE) 2016/679, **della fase di prima applicazione delle disposizioni sanzionatorie.**"

Ciò sta a significare che il Garante **per i primi otto mesi sarà più "clemente" nell'erogare le sanzioni,** operando una valutazione di tanti fattori, come peraltro era stato già indicato nelle Linee guida del Comitato europeo (ex WP29) del 3 ottobre 2017.

Le principali novità

Trattamento collegato ad un interesse pubblico non viene più inquadrato dal punto di vista soggettivo, ossia con riferimento all'appartenenza dei Titolari alla categoria di soggetti pubblici, **bensì da quello oggettivo** con riferimento alla finalità del trattamento.

- Una **specifica disciplina** viene introdotta per **il trattamento delle particolari categorie di dati** di cui all'art.9 del GDPR necessari per motivi di interesse pubblico rilevante;
- **Consenso del minore** per l'accesso ai servizi della società dell'informazione fissato a **14 anni;**
- **Introduzione del concetto di soggetti designati:** coloro ai quali all'interno dell'amministrazione sono affidati specifici compiti in merito al trattamento dei dati personali (responsabili interni e incaricati secondo la terminologia del previgente Codice);
- **Disciplina sanzionatoria articolata:** sanzioni ammnistrative previste dal Regolamento + Sanzioni penali in caso di trattamento illecito di dati.

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.

Per un'Amministrazione l'adeguamento al GDPR non è mai una banalità, perché bisogna rivedere l'organizzazione, l'informatica, la sicurezza, la modulistica, la formazione interna, l'informazione interna ed esterna, gli aspetti legali per il rapporto con gli Enti/Utenti/Cittadini, ecc

Che cosa serve fare?

NOMINARE IL RESPONSABILE DEL TRATTAMENTO

DOTARSI DI UNA FIGURA CHE VERIFICHI E GARANTISCA IL RISPETTO DELLE PROCEDURE : IL DATA PROTECTION OFFICER (DPO) O L'AMMINISTRATORE DELEGATO

VERIFICARE QUALI DATI PERSONALI VENGONO TRATTATI, CHI LI TRATTA, COME LI TRATTA E CON QUALI STRUMENTI («AS IS»)

ESEGUIRE DEGLI AUDIT PER VERIFICARE IL RISPETTO DELLE PROCEDURE

FORMARE IL PERSONALE PER RISPETTARE LE PROCEDURE

ADEGUARE GLI STRUMENTI SOFTWARE E NON (SISTEMI APPLICATIVI, INFRASTRUTTURE,HW/SW, SISTEMI DI SICUREZZA, ARCHIVI,..), AFFINCHÉ CONSENTANO DI RISPETTARE LE PROCEDURE

DEFINIRE LE PROCEDURE CHE STABILISCONO COME TRATTARE I DATI PERSONALI («TO BE»)

DIRITTO AL RISARCIMENTO E RESPONSABILITÀ (ART. 82)

GDPR

Chiunque subisca un danno materiale o immateriale causato da una violazione del regolamento ha il **diritto di ottenere il risarcimento** del danno dal Titolare o dal Responsabile del trattamento

Un Titolare del trattamento risponde per il danno cagionato dal suo trattamento che violi il regolamento

Il Responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del regolamento specificatamente diretti ai responsabili o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del Titolare

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

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

Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato

1. **natura, GRAVITÀ e durata DELLA VIOLAZIONE** tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;

2. carattere doloso o colposo della violazione;

3. **MISURE ADOTTATE** dal Titolare del trattamento o dal Responsabile del trattamento PER ATTENUARE IL DANNO subito dagli interessati;

4. grado di responsabilità del Titolare del trattamento o del Responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto;

5. **eventuali precedenti violazioni** pertinenti commesse dal Titolare del trattamento o dal Responsabile del trattamento;

6. **grado di cooperazione con l'autorità di controllo** al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;

7. categorie di dati personali interessate dalla violazione;

8. 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 (data breach);

9. 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;

10. l'adesione ai codici di condotta o ai meccanismi di certificazione;

11. 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).

Per le violazioni amministrative previste dal Regolamento …

… risponde sia il Titolare che il Responsabile del trattamento!

Nuove sanzioni amministrative (art. 83)

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

8 (*Consenso dei minori*)
11 (*Trattamento che non richiede l'identificazione*)
25 (*Protezione dei dati fin dalla progettazione*)
26 (*Contitolari del trattamento*)
27 (*Rappresentanti di titolari del trattamento non stabiliti nell'Unione*)
28 (*Responsabile del trattamento*)
29 (*Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento*)
30 (*Registri delle attività di trattamento*)
31 (*Cooperazione con l'autorità di controllo*)
32 (*Sicurezza del trattamento*)
33 (*Notifica di una violazione dei dati personali all'autorità di controllo*)
34 (*Comunicazione di una violazione dei dati personali all'interessato*)
35 (*Valutazione d'impatto sulla protezione dei dati*)
36 (*Consultazione preventiva*)
37 (*Designazione del responsabile della protezione dei dati*)
38 (*Posizione del responsabile della protezione dei dati*)
39 (*Compiti del responsabile della protezione dei dati*)
42 (*Certificazione*)
43 (*Organismi di certificazione*)
b) obblighi dell'organismo di certificazione a norma degli articoli 42 e 43;
c) obblighi dell'organismo di controllo a norma dell'articolo 41, paragrafo 4;

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

Nuove sanzioni amministrative

La violazione delle disposizioni seguenti è soggetta a sanzioni amministrative fino a 20 000 000 EUR, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

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

Fatti salvi i poteri correttivi delle autorità a norma dell'articolo 58, paragrafo 2, ogni Stato può prevedere norme che dispongano se e in quale misura possono essere inflitte sanzioni amministrative ad autorità pubbliche e organismi pubblici istituiti in tale Stato.
L'esercizio da parte dell'autorità dei poteri attribuitile dal presente articolo è soggetto a garanzie procedurali adeguate in conformità del diritto dell'Unione e degli Stati membri, inclusi il ricorso giurisdizionale

- Sanzioni **penali** quando previste dalla legge nazionale
- Sanzioni **pecuniarie**: saranno Efficaci, Proporzionate e Dissuasive

fino a **€ 10 milioni**
o al **2%** del fatturato
mondiale (se superiore)

- Es. Violazione obblighi in materia di consenso dei minori, misure di Sicurezza
- Es. Violazione obblighi impartiti dal Titolare
- Es. Violazione obblighi di comunicazione per Data Breach

Fino a **€ 20 milioni**
o al **4%** del fatturato
mondiale per le imprese (se superiore)

- Es. Violazioni concernenti i diritti degli interessati, i principi cardine
del trattamento (es. consenso) i trasferimenti ecc.
- Es. Violazioni di ordini o misure imposte dall'Autorità

GDPR

Cosa dobbiamo fare?

Cosa dobbiamo fare?

Documentare la conformità

Per dimostrare di essere conformi al GDPR è necessario **raccogliere la documentazione necessaria.** Le attività e i documenti posti in essere in ogni fase del Trattamento dovranno essere riesaminati e aggiornati regolarmente per assicurare una protezione dei Dati permanente

Cosa dobbiamo fare?

Per provare la conformità al Regolamento, predisporre e tenere aggiornata la documentazione necessaria.

- Documentazione attestante i trattamenti di dati personali svolti (**Registro delle attività di trattamento,** valutazione d'impatto, la documentazione prevista per il trasferimento dei dati Extra UE);
- Documentazione attestante il rispetto dei diritti e delle libertà dei soggetti interessati (**le informative, i moduli di raccolta consensi, l'attestazione dei consensi raccolti, la gestione dei diritti esercitati**);
- Documentazione che definisce i ruoli e le responsabilità in materia di protezione dei dati personali (i contratti e le nomine dei responsabili esterni, la gestione degli autorizzati/delegati al trattamento, le procedure interne, etc.);
- Comprova delle misure di sicurezza tecniche implementate (analisi dei log, report, configurazioni, policy, etc.).

Cosa dobbiamo fare?

Mappatura completa (pur se generica) del modus operandi:

- lettere di nomina degli autorizzati/incaricati e degli amministratori di sistema;
- clausole contrattuali con gli eventuali responsabili (esterni) del trattamento;
- informative (dipendenti, clienti, utenti/pazienti ecc.);
- modelli di informativa/consenso;
- DPS se adottato e mantenuto aggiornato;
- policy e/o regolamenti interni in materia di trattamento dei dati personali;
- registri/elenchi hardware e software;
- eventuali procedure certificate;
- etc….

Cosa dobbiamo fare?

Il Registro del trattamento...

- deve considerato come un **documento vivo, da tenere sempre aggiornato**. La mappatura all'inizio potrà concentrarsi solo su ciò che obbligatoriamente l'art. 30 prevede ma poi potrà via via ricomprendere tanti altri elementi utili per illustrare tutti i trattamenti sviluppati dalla struttura di riferimento, in modo da procedere con un approccio reale di accountability.

«Per dimostrare che si conforma al presente regolamento, il Titolare del trattamento o il Responsabile del trattamento dovrebbe tenere, un registro delle attività di trattamento effettuate sotto la sua responsabilità. Bisognerebbe obbligare tutti i titolari del trattamento e i responsabili del trattamento a cooperare con l'autorità di controllo e a mettere, su richiesta, detti registri a sua disposizione affinché possano servire per monitorare detti trattamenti».

Cosa dobbiamo fare?

Registro del Titolare del trattamento

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) 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, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
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 di cui all'articolo 32, paragrafo 1.

Il Registro del trattamento è da tenersi in forma scritta e anche in formato elettronico.

Cosa dobbiamo fare?

Registro del Responsabile del trattamento

a) il nome e i dati di contatto del Responsabile o dei responsabili del trattamento, di ogni Titolare del trattamento per conto del quale agisce il Responsabile del trattamento, del rappresentante del Titolare del trattamento o del Responsabile del trattamento e, ove applicabile, del Responsabile della protezione dei dati;
b) le categorie dei trattamenti effettuati per conto di ogni Titolare del trattamento;
c) 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, la documentazione delle garanzie adeguate;
d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

Il Registro del trattamento è da tenersi in forma scritta e anche in formato elettronico.

Cosa dobbiamo fare?

- **Censire tutti i trattamenti di dati personali effettuati**, tramite interviste con i responsabili dei vari processi amministrativi;
- individuare gli eventuali trasferimenti di dati personali verso paesi extra UE e verificare il rispetto delle disposizioni di cui agli artt. da 44 a 49 del GDPR;
- Raccogliere tutte le informazioni e la documentazione necessaria per la compilazione del registro dei trattamenti (es. applicazioni, servizi esternalizzati, sistemi di controllo dei dati, sistemi di log retention ecc.);
- Impostare il registro dei trattamenti e compilare le parti per le quali si è già in possesso delle necessarie informazioni;

Cosa dobbiamo fare?

- **Definire i contenuti dell'accordo con gli eventuali contitolari**;
- individuare, dopo aver verificato il possesso dei requisiti previsti dall'art. 28 del GDPR, i responsabili del trattamento e definire i contenuti vincolanti del contratto o altro atto giuridico;
- individuare gli eventuali referenti interni per la gestione delle politiche aziendali in materia di protezione dei dati personali;
- definire un sistema di controlli periodici (audit) che consentano il costante monitoraggio del livello di Compliance con il GDPR;
- definire un **piano formativo** su più livelli di competenze per garantire il rispetto dell'art. 29 del GDPR «*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*».

Cosa dobbiamo fare?

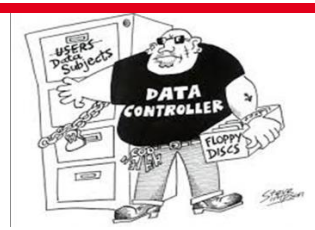
- aggiornare la documentazione esistente per renderla conforme al GDPR (es. informative, moduli di consenso, eventuali accordi con contitolari, eventuali contratti o altri atti giuridici con i responsabili esterni, policy aziendali);

- predisporre la documentazione mancante.

Cosa dobbiamo fare?

Dopo la mappatura sarà necessario (ex art. 24 e 32 del GDPR):

- **individuare i possibili ambiti di rischio** che dovranno essere oggetto di Valutazione;
- definire la metodologia di analisi dei rischi più adatta alla realtà Organizzativa con particolare riferimento ai sistemi informativi;
- analizzare (per ogni trattamento o per trattamenti simili) sia i rischi connessi ai trattamenti effettuati senza l'utilizzo di strumenti elettronici, che quelli relativi alla configurazione dei sistemi informativi e ai software utilizzati;
- **censire le attuali misure di sicurezza organizzative, fisiche e logiche;**
- definire le misure di sicurezza necessarie a ridurre il rischio entro un livello di accettabilità (es. pseudonimizzazione, cifratura ecc.);
- verificare tutti gli applicativi adottati e da adottare e avviare politiche di controllo in linea con i principi di privacy by design e privacy by default (art. 25 GDPR).

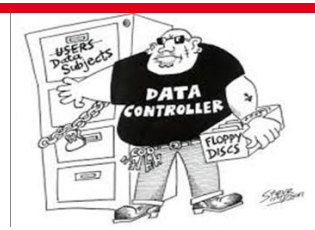


Cosa dobbiamo fare?

Sarà necessario concentrarsi anche sulle possibili violazioni nel trattamento di dati Personali (art. 33 e 34 GDPR):

- definire e integrare le procedure di incident management per la gestione dei DATA BREACH, in modo da ridurre il più possibile il termine che intercorre tra la violazione e il momento in cui ci si accorge della violazione
- implementare un sistema di file log che consenta la raccolta di tutte le necessarie informazioni a supporto delle violazioni e delle opportune indagini sottostanti;
- impostare il registro delle violazioni;
- definire la modulistica per le notificazioni all'autorità di Controllo e le comunicazioni agli interessati.

L'articolo 4 del Regolamento definisce il Data Breach come "violazione dei dati personali", ossia la violazione di 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 tale ambito la responsabilità del Titolare è duplice: (1) evitare che avvenga una violazione predisponendo e aggiornando le misure di sicurezza più e (2) in caso di violazione, adempiere tempestivamente a quanto prescritto dal Regolamento.



Cosa dobbiamo fare?

Gli obblighi connessi al Data Breach

Obbligo di notifica all'Autorità Garante "senza ingiustificato ritardo" e, ove possibile**, entro 72 ore** ex art. 33 del Regolamento Generale sulla Protezione dei Dati Personali.

Obbligo di comunicazione agli interessati quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

La notifica deve contenere:

- natura della violazione dei dati personali, ivi comprese le categorie e il numero di interessati nonché il tipo e il numero di record coinvolti.
- dati di contatto del Responsabile della protezione dei dati.
- descrizione delle probabili conseguenze della violazione.
- descrizione delle misure adottate o da adottare per porre rimedio alla violazione e contrastarne gli effetti

Cosa dobbiamo fare?

In base al principio di Accountability sarà indispensabile (ex art. 35 del GDPR):

- **individuare, i trattamenti per i quali è necessario effettuare la Valutazione d'impatto** (vedere elenco Garante);
- individuare la metodologia più appropriata da utilizzare per la valutazione d'impatto;
- effettuare la valutazione d'impatto per singoli trattamenti (o per gruppi simili che presentano rischi analoghi) nonché le necessarie misure tecniche ed organizzative per attenuarli;
- predisporre e conservare la documentazione relativa alla DPIA (Data Protection Impact Assessment);
- definire le modalità per il monitoraggio e l'eventuale revisione della DPIA

Informazioni e Istruzioni agli autorizzati

A tal fine, vengono fornite **INFORMAZIONI ED ISTRUZIONI** alle quali attenersi per l'assolvimento del compito assegnato:

- trattare i dati personali, in base all'art. 5 del GPDR, in modo lecito, corretto e trasparente e dovranno essere:
  - raccolti per finalità implicite e legittime e successivamente trattati in modo che non vi sia incompatibilità con tali finalità;
  - adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati");
  - esatti, e se necessario, aggiornati, adottando tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati ("esattezza");
  - conservati in una forma che consenta l'identificazione degli interessati per un periodo non superiore al conseguimento delle finalità per le quali sono trattati ("limitazione della conservazione");
  - trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche ed organizzative adeguate ("integrità e riservatezza");

- svolgere le attività previste dai trattamenti **secondo le direttive del Responsabile del trattamento dei dati**; non modificare i trattamenti esistenti **o introdurre nuovi trattamenti senza l'esplicita autorizzazione** del Responsabile del trattamento dei dati;

Informazioni e Istruzioni agli autorizzati

- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- informare il Responsabile in caso di incidente di sicurezza che coinvolga dati particolari (ex Sensibili) e non;
- raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
- eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge;
- recepire nuove indicazioni fornite dal Titolare del Trattamento **anche partecipando a percorsi formativi quando previsti;**
- assicurare la **riservatezza** opportuna e necessaria affinché il trattamento dei dati, sia effettuato in conformità alle disposizioni del GDPR e del D.lgs 196/2003 s.m.i. e volte alla prevenzione da parte del Titolare dei crimini informatici e del trattamento illecito di dati;

Informazioni e Istruzioni agli autorizzati

- trattare i dati personali, eventualmente riferiti a **categorie particolari** (art. 9) o relativi a condanne penali e reati (art. 10) è ammesso se lecito (art. 6) e cioè quando:

  - l'interessato ha espresso il consenso al trattamento dei propri dati personali;
  - 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;
  - il trattamento è necessario per adempiere ad un obbligo di legge cui è tenuto il Titolare o per salvaguardare gli interessi vitali dell'interessato;
  - il trattamento è necessario per il perseguimento del legittimo interesse del Titolare;

- **garantire all'interessato l'esercizio dei diritti** sui propri dati secondo quanto previsto dal GDPR (es: diritto di accesso, di rettifica, di limitazione, di portabilità, di opposizione, ecc.);

Informazioni e Istruzioni agli autorizzati

Inoltre:

- **è consentita la trasmissione di dati all'interno dell'organico del Titolare** per i compiti ed i fini stabiliti dallo stesso, agendo sotto la sua diretta autorità, allo stesso modo sono autorizzati i trattamenti di dati pseudonimizzati;

- È vietata ogni comunicazione/diffusione di dati verso l'esterno dell'Amministrazione e/o Organizzazione senza preventiva autorizzazione del Titolare stesso o del Responsabile; il divieto permane anche dopo la cessazione dell'incarico e/o del rapporto di lavoro;

- nessun dato deve essere comunicato a soggetti identificati esterni all'Amministrazione e/o Organizzazione o diffuso (trasmesso a soggetti indeterminati), senza specifica autorizzazione del Responsabile del Trattamento; è vietata la diffusione dei dati trattati ed in particolare di quelli sensibili;

- sono consentite le comunicazioni di dati che avvengono nell'ambito di un rapporto contrattuale/convenzionale instaurato dall'Amministrazione con terzi per l'esternalizzazione di attività/funzioni/servizi, **a condizione che il terzo sia stato nominato Responsabile esterno del trattamento dei dati;**

- l'incarico conferito autorizza l'accesso agli archivi contenenti atti e documenti riportanti dati personali comuni e al trattamento di questi; l'accesso ed il trattamento dati vanno limitati alle necessità per l'adempimento dei compiti da assolvere;

- per il tempo necessario allo svolgimento delle operazioni di trattamento si dovrà diligentemente controllare e custodire gli atti e documenti contenenti dati personali per evitare visione, possesso, utilizzo non autorizzati;

Informazioni e Istruzioni agli autorizzati

- astenersi dall'effettuare operazioni di trattamento dei dati personali, di cui si a conoscenza durante lo svolgimento dell'incarico, evitare di conservarli, duplicarli, comunicarli o cederli ad altri, dopo la cessazione del rapporto di lavoro;

- **in caso di interruzione, anche temporanea, del lavoro verificare che i dati trattati non siano accessibili a terzi non autorizzati;**

- informare tempestivamente il Responsabile del trattamento di ogni questione rilevante in relazione al trattamento di dati personali effettuato e di eventuali richieste pervenute dagli interessati;

- nel caso in cui si constati o si sospetti un disguido o un incidente che abbia messo o possa mettere a repentaglio la sicurezza dei dati trattati, darne immediata comunicazione al Responsabile del trattamento;

- segnalare al Responsabile eventuali circostanze, che richiedano il necessario ed opportuno aggiornamento delle misure di sicurezza adottate, al fine di ridurre al minimo i rischi di diffusione, distruzione o perdita anche accidentale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;

Informazioni e Istruzioni agli autorizzati

- fornire al Titolare o al Responsabile, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire loro una adeguata azione di controllo;

- **non trasmettere dati particolari (sensibili) via e-mail.** Nel caso in cui sia strettamente necessaria tale forma di trasmissione per ragioni d'ufficio, occorrerà porre in essere gli accorgimenti atti ad impedire la visione del contenuto del file da parte di soggetti non autorizzati o non legittimati al trattamento, che siano diversi dai destinatari delle comunicazioni elettroniche. In particolare, si raccomanda il ricorso all'uso di tecniche di criptazione o di cifratura dei messaggi, ovvero il ricorso all'uso di codificazione dei dati contenuti nel testo delle comunicazioni;

- rispettare, se presente, il documento sulla sicurezza dei dati, predisposto dall'Amministrazione e/o dall'Organizzazione;

- **non alterare in alcun modo la configurazione software della stazione di lavoro**, evitando di installare qualunque software sconosciuto o non approvato;

- **non utilizzare la rete dell'Amministrazione e/o Organizzazione per fini non espressamente autorizzati**;

- è vietato l'utilizzo improprio di documenti, dati, informazioni a qualsiasi titolo posseduti, ricevuti o trasmessi;

Informazioni e Istruzioni agli autorizzati

Con riferimento alle misure di sicurezza, le PERSONE AUTORIZZATE AL TRATTAMENTO O INCARICATI:

- accedono al sistema informativo per **mezzo di credenziali di autenticazione;** le credenziali di autenticazione consistono in un codice (user id o username) per l'identificazione dell'incaricato, associata ad una parola chiave (password) conosciuta solo dall'incaricato;

- utilizzano la **password con una lunghezza minima di otto caratteri, sia numerici che alfabetici** (o, se il programma in uso non lo permette, dal numero massimo di caratteri consentito);

- nella generazione della password non utilizzano elementi o notizie a loro facilmente riconducibili;

- **modificano la password** al primo utilizzo, ogni volta che viene richiesto dal sistema (al massimo 6 mesi, 3 mesi se i dati trattati sono sensibili (ad. es. di salute) e/o giudiziari) e nel caso vi sia il dubbio che la stessa password abbia perso il carattere di segretezza;

- qualora il sistema non renda obbligatoria la modifica della password nel rispetto dei predetti termini, **l'utilizzatore provvede autonomamente a tale variazione;**

- adottano particolari cautele per assicurare la segretezza della password (evitare la digitazione in presenza di terzi, conservarne i riferimenti in luogo non accessibile a terzi);

Informazioni e Istruzioni agli autorizzati

Con riferimento alle misure di sicurezza, le PERSONE AUTORIZZATE AL TRATTAMENTO O INCARICATI:

- nel caso di allontanamento dalla propria postazione di lavoro, **l'incaricato adotta tutte le cautele necessarie atte ad evitare l'accesso ai dati personali trattati o in trattamento sia cartaceo che automatizzato da parte di terzi**, anche se dipendenti, a meno che non siano autorizzati;
- **non lasciano la propria stazione di lavoro incustodita e collegata con il proprio account (nome utente) e password all'ambiente di rete;**

- bloccano la propria stazione di lavoro durante la pausa pranzo, ovvero in tutte le occasioni in cui ci si assenti dall'ufficio; nel caso in cui fosse necessario mantenere accesa la stazione di lavoro, utilizzare i metodi messi a disposizione dal sistema per bloccare la stessa, come ad esempio il blocco sessione o il salvaschermo con password;

- per le banche dati automatizzate utilizzano il proprio codice di accesso personale, evitando di operare su terminali altrui e/o lasciare aperto il sistema operativo con la propria password inserita, in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;

- tenere un comportamento corretto durante la navigazione in internet, così come previsto dalle disposizioni interne sulla modalità di utilizzo dei servizi di rete.

Informazioni e Istruzioni agli autorizzati

Con riferimento alla gestione dei dati personali su supporto cartaceo, le PERSONE AUTORIZZATE AL TRATTAMENTO O INCARICATI:

- devono garantire sempre la corretta custodia degli stessi; i documenti non devono essere lasciati incustoditi sulla propria scrivania e/o in luoghi aperti al pubblico in assenza di altri incaricati addetti al medesimo trattamento; non devono essere consultati da altri incaricati non abilitati al trattamento; non possono essere riprodotti o fotocopiati se non per esigenze connesse alla finalità del trattamento;

- devono conservare i documenti o gli atti che contengono dati sensibili e/o giudiziari in archivi ad accesso controllato (armadi/schedari/contenitori muniti di serratura oppure soggetti a sorveglianza da parte di personale preposto);

- al termine delle operazioni di trattamento, devono, restituire tempestivamente la documentazione prelevata dagli archivi;

- in caso di utilizzo di stampante, fotocopiatrice o fax condivisi da vari utenti e collocati al di fuori dei locali ove è posta la singola stazione di lavoro, le stampe devono essere immediatamente raccolte e custodite con le modalità sopra descritte;

- non devono gettare via copie cartacee contenenti dati personali, senza averle distrutte prima in modo opportuno;

- devono adottare misure che siano idonee a limitare la conoscenza dei dati sensibili qualora essi siano presenti nei flussi documentali dell'Amministrazione garantendo il rispetto della riservatezza dei dati degli interessati.

GRAZIE a tutti per l'attenzione