invictusaziende

il metodo vincente per l'adeguamento privacy

# Manuale

## delle domande e delle terminologie tecniche.

## Indice

## 1. Definizioni terminologiche del regolamento:

Ai fini del presente regolamento s'intende per:

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; (C26, C27, C30)

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**;

3) «**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro; (C67)

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. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

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 e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

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;

13) «**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;

14) «**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;

15) «**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;

## 1. Quando esistono i fondamenti di 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 privacy - D.Lgs. 196/2003 (**consenso**, **adempimento obblighi contrattuali**, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati).

## 2. Quali sono le condizioni per il consenso?

**1.** 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.

## 3. Quali sono i contenuti dell'informativa?

I contenuti dell'informativa sono i seguenti:

**1.** il titolare deve sempre specificare i dati di contatto del **RPD-DPO** (Responsabile della protezione dei dati - Data Protection Officer), ove esistente,

**2.** la base giuridica del trattamento

**3.** qual'è il suo interesse legittimo se quest'ultimo costituisce **la base giuridica del trattamento**,

**4.** se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti (esempio: si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; si utilizzano BCR di gruppo; sono state inserite specifiche clausole contrattuali modello, ecc.). Il regolamento prevede anche ulteriori informazioni in quanto "**necessarie per garantire un trattamento corretto e trasparente**" in particolare:

**1.** il titolare deve specificare il periodo di **conservazione dei dati** o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di presentare un reclamo all'autorità di controllo.

**2.** se il trattamento comporta processi decisionali automatizzati (anche la **profilazione**), l'informativa deve specificarlo e deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.

## 4. Quali sono le condizioni per il consenso nei confronti dei minori?

**1.** Per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati persona li del minore è **lecito ove il minore abbia almeno 16 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.

**2.** Il titolare del trattamento si adopera in ogni modo ragionevole per verificare in tali casi che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili.

**3.** Il paragrafo 1 non pregiudica le disposizioni generali del diritto dei **contratti degli Stati membri**, quali le norme sulla validità, la formazione o l'efficacia di un contratto rispetto a un minore.

## 1. Cosa è il registro delle attività di trattamento?

L'art. 30 del Regolamento (EU) n. 679/2016 (di seguito "GDPR") prevede tra gli adempimenti principali del titolare e del responsabile del trattamento la tenuta del registro delle attività di trattamento.

E' un documento contenente le principali informazioni (specificatamente individuate dall'art. 30 del GDPR) relative alle operazioni di trattamento svolte dal titolare e, se nominato, dal **responsabile** del trattamento (sul registro del responsabile, vedi, in particolare, il punto 6).
Costituisce uno dei principali elementi di **accountability** del titolare, in quanto strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, indispensabile per ogni attività di valutazione o analisi del rischio e dunque preliminare rispetto a tali attività. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

## 2. Chi è tenuto a redigere il registro delle attività?

Tutti i titolari e i responsabili del trattamento sono tenuti a redigere il Registro delle attività di trattamento In particolare, in ambito privato, i soggetti obbligati sono così individuabili: imprese o organizzazioni **con almeno 250 dipendenti**; qualunque **titolare** o **responsabile** (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti che possano **presentare un rischio** – anche non elevato – per i diritti e le libertà dell'interessato; qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti non occasionali; qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti delle categorie particolari di dati di cui all'art 9, paragrafo 1 GDPR, o di dati personali relativi a condanne penali e a reati di cui all'art. 10 GDPR.

## 3. Quali informazioni deve contenere il registro delle attività?

Il Regolamento individua dettagliatamente le informazioni che devono essere contenute nel registro delle attività di trattamento del titolare (art. 30, par. 1 del GDPR) e in quello del responsabile (art. 30, par. 2 del GDPR). Con riferimento ai contenuti si rappresenta quanto segue:

**A**. nel campo "**finalità del trattamento**" oltre alla precipua indicazione delle stesse, distinta per tipologie di trattamento (es. trattamento dei dati dei dipendenti per la gestione del rapporto di lavoro; trattamento dei dati di contatto dei fornitori per la gestione degli ordini), sarebbe opportuno indicare anche la base giuridica dello stesso (v. art. 6 del GDPR; in merito, con particolare riferimento al "**legittimo interesse**", si rappresenta che il registro potrebbe riportare la descrizione del legittimo interesse concretamente perseguito, le "**garanzie adeguate**" eventualmente approntate, nonché, ove effettuata, la preventiva valutazione d'impatto posta in essere dal titolare. Sempre con riferimento alla base giuridica, sarebbe parimenti opportuno: in caso di trattamenti di "categorie particolari di dati", indicare una delle condizioni di cui all'art. 9, par. 2 del GDPR; in caso di trattamenti di dati relativi a condanne penali e reati, riportare la specifica normativa (nazionale o dell'Unione europea) che ne autorizza il trattamento ai sensi dell'art. 10 del GDPR;

**B**. nel campo "**descrizione delle categorie di interessati e delle categorie di dati personali**" andranno specificate sia le **tipologie di interessati** (es. clienti, fornitori, dipendenti) sia quelle di dati personali oggetto di trattamento (es. dati anagrafici, dati sanitari, dati biometrici, dati genetici, dati relativi a condanne penali o reati, ecc.);

**C**. nel campo "**categorie di destinatari a cui i dati sono stati o saranno comunicati**" andranno riportati, anche semplicemente per categoria di appartenenza, gli altri titolari cui siano comunicati i dati (es. enti previdenziali cui debbano essere trasmessi i dati dei dipendenti per adempiere agli obblighi contributivi). Inoltre, si ritiene opportuno che siano indicati anche gli eventuali altri soggetti ai quali, in qualità di responsabili e **sub-responsabili** del trattamento, siano trasmessi i dati da parte del titolare (es. soggetto esterno cui sia affidato dal titolare il servizio di elaborazione delle buste paga dei dipendenti o altri soggetti esterni cui siano affidate in tutto o in parte le attività di trattamento).
Ciò al fine di consentire al titolare medesimo di avere effettiva contezza del novero e della tipologia dei soggetti esterni cui sono affidate le operazioni di trattamento dei dati personali;

**D**. nel campo "**trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale**" andrà riportata l'informazione relativa ai suddetti trasferimenti unitamente all'indicazione relativa al Paese/i terzo/i cui i dati sono trasferiti e alle "garanzie" adottate ai sensi del capo V del GDPR (es. decisioni di adeguatezza,

norme vincolanti d'impresa, clausole contrattuali tipo, ecc.);
**E**. nel campo "**termini ultimi previsti per la cancellazione delle diverse categorie di dati**" dovranno essere individuati i tempi di cancellazione per tipologia e finalità di trattamento (ad es. "in caso di rapporto contrattuale, i dati saranno conservati per 10 anni dall'ultima registrazione – v. art. 2220 del codice civile"). Ad ogni modo, ove non sia possibile stabilire a priori un termine massimo, i tempi di conservazione potranno essere specificati mediante il riferimento a criteri (es. norme di legge, prassi settoriali) indicativi degli stessi (es. "in caso di contenzioso, i dati saranno cancellati al termine dello stesso");

**F**. nel campo "**descrizione generale delle misure di sicurezza**" andranno indicate le misure tecnico-organizzative adottate dal titolare ai sensi dell'art. 32 del GDPR tenendo presente che l'elenco ivi riportato costituisce una lista aperta e non esaustiva, essendo rimessa al titolare la valutazione finale relativa al livello di sicurezza adeguato, caso per caso, ai rischi presentati dalle attività di trattamento concretamente poste in essere. Tale lista ha di per sé un carattere dinamico (**e non più statico come è stato per l'Allegato B del D. Lgs. 196/2003** ) dovendosi continuamente confrontare con gli sviluppi della tecnologia e l'insorgere di nuovi rischi. Le misure di sicurezza possono essere descritte in forma riassuntiva e sintetica, o comunque idonea a dare un quadro generale e complessivo di tali misure in relazione alle attività di trattamento svolte, con possibilità di fare rinvio per una valutazione più dettagliata a documenti esterni di carattere generale (es. procedure organizzative interne; security policy ecc.).

## 1. Chi è l'RDP/ DPO?

Il regolamento generale sulla protezione dei dati GDPR (General Data Protection Regulation) che esplicherà i propri effetti a partire dal 25 maggio 2018, offre un quadro di riferimento in termini di compliance per la protezione dei dati in Europa, aggiornato e fondato sul principio di responsabilizzazione (**accountability**). Gli RPD/DPO (Responsabile della protezione dei dati - Data Protection Officer) saranno al centro di questo nuovo quadro giuridico in molti ambiti, e saranno chiamati a facilitare l'osservanza delle disposizioni del GDPR. In base al GDPR, alcuni titolari e responsabili del trattamento sono tenuti a nominare un DPO in via obbligatoria.

Ciò vale per tutte le autorità pubbliche e tutti i soggetti pubblici, indipendentemente dai dati oggetto di trattamento, e per altri soggetti che, come attività principale, effettuino un monitoraggio regolare e su "larga scala" delle persone fisiche ovvero trattino su "larga scala" categorie particolari di dati personali (dati sensibili). Anche ove il regolamento non imponga in modo specifico la designazione di un DPO, può risultare utile procedere a tale designazione su base volontaria. Il Gruppo di lavoro "articolo 29" (WP29) incoraggia gli approcci di questo genere.

La figura del DPO non costituisce una novità assoluta. **La direttiva 95/46/CE3** non prevedeva alcun obbligo di nomina di un DPO, ma in molti Stati membri questa è divenuta una prassi nel corso degli anni. Ancor prima dell'adozione del GDPR, il WP29 ha sostenuto che questa figura rappresenti un elemento fondante ai fini della responsabilizzazione, e che la nomina del DPO possa facilitare l'osservanza della normativa e aumentare il margine competitivo delle imprese.

Oltre a favorire l'osservanza attraverso strumenti di **accountability** (per esempio, supportando valutazioni di impatto e conducendo o supportando audit in materia di protezione dei dati), i **DPO** fungono da interfaccia fra i soggetti coinvolti: autorità di controllo, interessati, divisioni operative all'interno di un'azienda o di un ente. I DPO non rispondono personalmente in caso di inosservanza del GDPR. Quest'ultimo chiarisce che spetta al titolare o al responsabile del trattamento garantire ed essere in grado di dimostrare che le operazioni di trattamento sono conformi alle disposizioni del regolamento stesso (articolo 24, primo paragrafo).

L'onere di assicurare il rispetto della normativa in materia di protezione dei dati ricade sul titolare o sul responsabile. Inoltre, al titolare o al responsabile del trattamento spetta il compito fondamentale di consentire lo svolgimento efficace dei compiti cui il DPO è preposto. La nomina di un DPO è solo il primo passo, perché il DPO deve disporre anche di autonomia e risorse sufficienti a svolgere in modo efficace i compiti cui è chiamato. Il GDPR riconosce nel DPO uno degli elementi chiave all'interno del **nuovo sistema di governance dei dati**, e prevede una serie di condizioni in rapporto alla nomina, allo status e ai compiti specifici.

## 2. Quando è richiesta la nomina del RPD/DPO?

La designazione di un DPO è obbligatoria:

**1**. se il trattamento è svolto da un'**autorità pubblica** o da un **organismo pubblico**;

**2**. se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il **monitoraggio regolare** e sistematico di interessati su **"larga scala"**.

**3**. se le attività principali del titolare o del responsabile consistono nel trattamento **su "larga scala"** di categorie particolari di dati o di dati personali relativi a condanne penali e reati.

Si tenga presente che la designazione obbligatoria di un DPO può essere prevista anche in casi ulteriori in base alla legge nazionale o al diritto dell'UE. Inoltre, anche ove la designazione di un DPO non sia obbligatoria, può risultare utile procedere a tale designazione su base volontaria. Il Gruppo di lavoro "Articolo 29" (WP29) incoraggia un approccio di questo genere. Qualora si proceda alla designazione di un DPO su base volontaria, si applicano gli identici requisiti – in termini di criteri per la designazione, posizione e compiti – che valgono per i DPO designati in via obbligatoria.

## 3. Cosa significa "attività principali"?

Con "attività principali" si possono intendere le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal titolare o dal responsabile del trattamento, comprese tutte quelle attività per le quali il trattamento dei dati è inscindibilmente connesso all'attività del titolare o del responsabile. Per esempio, il trattamento di dati relativi alla salute (**come le cartelle sanitarie dei pazienti**) è da ritenersi una delle attività principali di qualsiasi ospedale; ne deriva che tutti gli ospedali dovranno designare un DPO.

D'altra parte, tutti gli organismi (pubblici e privati) svolgono determinate attività quali il pagamento delle retribuzioni al personale ovvero dispongono di strutture standard di supporto informatico. Si tratta di esempi di funzioni di supporto necessarie ai fini dell'attività principale o dell'oggetto principale del singolo organismo, ma pur essendo necessarie o perfino essenziali sono considerate solitamente di natura accessoria e non vengono annoverate fra le attività principali.

## 4. Cosa significa "su larga scala"?

Il regolamento non definisce cosa rappresenti un trattamento "su larga scala".
Il WP29 raccomanda di tenere conto, in particolare, dei fattori qui elencati al fine di stabilire se un trattamento sia effettuato su "larga scala":

**1**. il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
**2**. il volume dei dati e/o le diverse **tipologie** di dati oggetto di trattamento;
**3**. la durata, ovvero la **persistenza**, dell'attività di trattamento;
**4**. la **portata geografica** dell'attività di trattamento.

Alcuni esempi di trattamento su "larga scala" sono i seguenti:
**A**. trattamento di dati relativi a pazienti svolto da un **ospedale** nell'ambito delle ordinarie attività;
**B**. trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (per esempio, il **loro tracciamento** attraverso titoli di viaggio);
**C**. trattamento di dati di **geolocalizzazione** raccolti in tempo reale per finalità statistiche da un responsabile specializzato nella prestazione di servizi di questo tipo rispetto ai clienti di una catena internazionale di fast food;
**D**. trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o di una banca nell'ambito delle ordinarie attività;
**E**. trattamento di dati personali da parte di un motore di ricerca per finalità di **pubblicità comportamentale**;
**F**. trattamento di dati (**metadati**, **contenuti**, **ubicazione**) da parte di fornitori di servizi telefonici o telematici.
Altri esempi di trattamento su "non su larga scala" sono i seguenti:
**A**. trattamento di dati relativi a pazienti svolto da un singolo professionista sanitario;
**B**. trattamento di dati personali relativi a condanne penali e reati svolto da un singolo avvocato.

## 5. Cosa significa "monitoraggio regolare e sistematico"?

Il concetto di monitoraggio regolare e sistematico degli interessati non trova definizione all'interno del GDPR; tuttavia, esso comprende senza dubbio tutte le forme di tracciamento e **profilazione** su Internet anche per finalità di pubblicità comportamentale.
Non si tratta, però, di un concetto riferito esclusivamente all'ambiente online. Alcune esemplificazioni di attività che possono configurare un monitoraggio regolare e sistematico di interessati: curare il funzionamento di una rete di telecomunicazioni;

la prestazione di servizi di telecomunicazioni; il **reindirizzamento** di messaggi di posta elettronica; attività di marketing basate sull'analisi dei dati raccolti; profilazione e scoring per finalità di valutazione del rischio (per esempio, a fini di valutazione del rischio creditizio, definizione dei premi assicurativi, prevenzione delle frodi, accertamento di forme di riciclaggio); tracciamento dell'ubicazione, per esempio da parte di app su dispositivi mobili; programmi di fidelizzazione; pubblicità comportamentale; monitoraggio di dati relativi allo stato di benessere psicofisico, alla forma fisica e alla salute attraverso dispositivi indossabili; utilizzo di telecamere a circuito chiuso; dispositivi connessi quali contatori intelligenti, automobili intelligenti, dispositivi per la domotica, ecc.

## 6. Dove dovrebbe collocarsi il DPO?

Per garantire l'accessibilità del DPO, il WP29 raccomanda la sua collocazione nel territorio dell'Unione europea, indipendentemente dall'esistenza di uno stabilimento del titolare o del responsabile nell'UE. Tuttavia, non si può escludere che un DPO sia in grado di adempiere ai propri compiti con **maggiore efficacia** operando al di fuori dell'UE in alcuni casi ove titolare o responsabile non sono stabiliti nel territorio dell'Unione europea.

## 7. DPO può essere un soggetto esterno?

SI. Il DPO può far parte del personale del titolare o del responsabile del trattamento (DPO interno) ovvero "**assolvere** i suoi compiti in base a un contratto di servizi". In quest'ultimo caso il DPO sarà esterno e le sue funzioni saranno esercitate sulla base di un contratto di servizi stipulato con una persona fisica o giuridica.
Se la funzione di DPO é svolta da un fornitore esterno di servizi, i compiti stabiliti per il DPO potranno essere assolti efficacemente da un team operante sotto l'autorità di un contatto principale designato è "responsabile" per il singolo cliente. In tal caso, é indispensabile che ciascun soggetto appartenente al fornitore esterno operante quale DPO soddisfi tutti i requisiti applicabili come fissati nel GDPR.

Per favorire efficienza e correttezza e prevenire **conflitti di interesse** a carico dei

componenti il team, le linee-guida raccomandano di procedere a una chiara ripartizione dei compiti nel team del DPO esterno, attraverso il contratto di servizi, e di prevedere che sia un solo soggetto a fungere da contatto principale e "incaricato" per ciascun cliente.

## 1. Quali sono le modalità ed i tempi per l'esercizio dei diritti da parte dell'interessato?

Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), **1 mese**, estendibile fino a 3 mesi in casi di particolare complessità; il titolare deve comunque dare un riscontro all'interessato **entro 1 mese dalla richiesta**, anche in caso di diniego.

Spetta al titolare valutare la complessità del riscontro all'interessato e stabilire l'ammontare dell'eventuale contributo da chiedere all'interessato, ma soltanto se si tratta di richieste manifestamente infondate o eccessive (anche ripetitive) (art.12, paragrafo 5), a differenza di quanto prevedono gli art. 9, comma 5, e 10, commi 7 e 8, del Codice, ovvero se sono chieste più "copie" dei dati personali nel caso del diritto di accesso (art. 15, paragrafo 3); in quest'ultimo caso il titolare deve tenere conto dei costi **amministrativi sostenuti**. Il riscontro all'interessato di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano **l'accessibilità**; può essere dato oralmente solo se così richiede l'interessato stesso (art. 12, paragrafo 1; si veda anche art. 15, paragrafo 3).

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

## 2. Cosa si intende per diritto di acceso da parte dell'interessato?

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

Fra le informazioni che il titolare deve fornire non rientrano le "**modalità**" del trattamento, mentre occorre indicare il periodo di conservazione previsto o, se non è possibile, i criteri utilizzati per definire tale periodo, nonché le garanzie applicate in caso di trasferimento dei dati verso **Paesi terzi**.

## 3. Cosa si intende per diritto all'oblio?

Il diritto cosiddetto "**all'oblio**" si configura come un **diritto alla cancellazione dei propri dati personali in forma rafforzata**. Si prevede, infatti, l'obbligo per i titolari (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, pubblicandoli su un sito web) di **informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati**, compresi "qualsiasi link, copia o riproduzione" (si veda art. 17, paragrafo 2).
Ha un campo di applicazione più esteso di quello di cui all'art. 7, comma 3, lettera b), del Codice, poiché l'interessato ha il diritto di chiedere la cancellazione dei propri dati, per esempio, anche dopo revoca del consenso al trattamento (si veda art. 17, paragrafo 1).

## 4. Cosa si intende per diritto di limitazione al trattamento?

Si tratta di un diritto diverso e **più esteso rispetto al "blocco"** del trattamento di cui all'art. 7, comma 3, lettera a), del Codice: in particolare, è **esercitabile non solo in caso di violazione dei presupposti di liceità** del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì anche se l'interessato chiede la rettifica dei dati (in attesa di tale rettifica da parte del titolare) o si oppone al loro trattamento ai sensi dell'art. 21 del regolamento (in attesa della valutazione da parte del titolare).
Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la limitazione è vietato a meno che ricorrano determinate circostanze (consenso dell'interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra persona fisica o giuridica, interesse pubblico rilevante).

## 5. Cosa si intende per diritto alla portabilità dei dati?

Si tratta di uno dei nuovi diritti previsti dal regolamento, anche **se non è del tutto sconosciuto ai consumatori** (si pensi alla **portabilità** del numero telefonico).
**Non si applica ai trattamenti non automatizzati** (quindi non si applica agli archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio; in particolare, sono portabili solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare, per esempio), e solo i dati che siano stati "forniti" dall'interessato al titolare. Inoltre, il titolare deve essere in grado di **trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato**, se tecnicamente possibile.

## 1. Quali sono le principali modiche relative alle figure del Titolare e del Responsabile incaricato?

Le novità sono la disciplina della contitolarità del trattamento (art. 26) e impone ai titolari di definire specificamente (con un atto giuridicamente valido ai sensi del diritto nazionale) il rispettivo **ambito di responsabilità** e i compiti con particolare riguardo all'esercizio dei diritti degli interessati, che hanno comunque la possibilità di rivolgersi indifferentemente a uno **qualsiasi dei titolari operanti congiuntamente**.

Fissa più dettagliatamente (rispetto all'art. 29 del Codice) le caratteristiche dell'atto con cui il titolare designa un responsabile del trattamento attribuendogli specifici compiti: deve trattarsi, infatti, di un **contratto** (o **altro atto giuridico conforme al diritto nazionale**) e deve disciplinare tassativamente almeno le materie riportate al paragrafo 3 dell'art. 28 al fine di dimostrare che il responsabile fornisce "**garanzie sufficienti**" – quali, in particolare, la natura, durata e finalità del trattamento o dei trattamenti assegnati, le **categorie di dati oggetto di trattamento**, le **misure tecniche e organizzative adeguate** a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel regolamento;

La novità inoltre è rappresentata dalle nuove figure che sostituiscono gli incaricati, il responsabile infatti può nominare sub-responsabili del trattamento (si veda art. 28, paragrafo 4), per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario; **quest'ultimo risponde dinanzi al titolare dell'inadempimento dell'eventuale sub-responsabile**, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri

che l'evento dannoso "non gli è in alcun modo imputabile" (si veda art. 82, paragrafo 1 e paragrafo 3);

## 2. Quali sono gli altri obblighi previsti per il responsabile?

Prevede obblighi specifici in capo ai responsabili del trattamento, in quanto distinti da quelli pertinenti ai rispettivi titolari. Ciò riguarda, in particolare, la **tenuta del registro dei trattamenti svolti** (ex art. 30, paragrafo 2); l'adozione di idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti (ex art. 32 regolamento); la designazione di un RPD-DPO, nei casi previsti dal regolamento o dal diritto nazionale (si veda art. 37 del regolamento). Si ricorda, inoltre, che anche il responsabile non stabilito nell'UE dovrà **designare un rappresentante in Italia** quando ricorrono le condizioni di cui all'art. 27, paragrafo 3, del regolamento – diversamente da quanto prevede oggi l'art. 5, comma 2, del Codice.

## 1. Quali sono gli adempimenti previsti se tratto dati su base informatica?

Il regolamento pone con forza l'accento sulla "**responsabilizzazione**" (**accountability** nell'accezione inglese) di titolari e responsabili – ossia, sull'adozione di **comportamenti proattivi** e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento.

Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

Dipende dalla tipologia dei dati nel caso in cui il trattamento verta su dati personali le procedure saranno le seguenti: **A**. la **pseudonimizzazione** e la **cifratura** dei dati personali (con **pseudonimizzazione** si intende il processo informatico per il discernimento del dato dall'interessato in modo tale da non renderlo identificabile univocamente **esempio 1**, mentre la cifratura permette di rendere non in chiaro un dato mediante un processo informatico **esempio 2**)

**B**. la capacità di assicurare su base permanente la **riservatezza**, l'**integrità**, la **disponibilità** e la **resilienza** dei sistemi e dei servizi di trattamento;

**C**. la capacità di **ripristinare tempestivamente la disponibilità** e l'accesso dei dati personali in caso di incidente fisico o tecnico quindi politiche e procedure di "**disaster recovery**" che permettano di rendere nuovamente disponibile il dato.

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

## pseudonimizzazione esempio 1.

**Andrea Rossi**
ARTFGW56D34K5
Patologia X

Unico archivio

**Andrea Rossi**

ARTFGW56D34K5

Patologia X

Più archivi non collegati

## cifratura esempio 2.

**Andrea Rossi**
ARTFGW56D34K5
Patologia X

Dato viene cifrato

010001001010010

Dato non in chiaro

## 2. Quali sono gli adempimenti previsti se tratto dati su base cartacea?

Il regolamento come abbiamo più volte detto pone al centro il principio di **responsabilizzazione**, il nuovo **decreto legislativo n° 101 del 09/09/18** invece abroga l'allegato B all'interno del quale erano contenute le misure minime di sicurezza. In questa situazione si rende necessaria un'analisi di rischi per valutare esatta corrispondenza dei mezzi idonei a fronteggiare i rischi emergenti nel trattamento, **pur abrogando l'allegato B** ma ricorrendo ai principi di responsabilizzazione alcune linee guida dell'allegato B saranno utili per questa casistica in particolare:

**1**. In caso di trattamento di **dati sensibili** si riterrà necessario **utilizzo di zona non operativa**, segnalando la stessa con apposito cartello, all'interno della quale ci sia posizionato un registro dove firmeranno coloro i quali non rivestano le figure di responsabile o sub responsabile al trattamento. Per garantire i principi sanciti dall'art.32 del regolamento europeo cioè la **riservatezza**, l'**integrità**, la **disponibilità** e la **resilienza** dei sistemi e dei servizi di trattamento i dati verranno archiviati in armadi ignifughi che possano garantire l'integrità dei dati, e la **disponibilità** degli stessi che potrà essere garantita mediante scansione digitale (anche se poi andrebbero pnesudonimizzati e cifrati), la **riservatezza** sarebbe garantita dal locale riservato, la **resilienza** è tipica dei sistemi informatici quindi non può essere traslata sui sistemi cartacei.

**2**. In caso di trattamento di **dati personali** sempre su supporti cartaceo invece i principi di **riservatezza**, l'**integrità**, la **disponibilità** e la **resilienza** saranno osservati in maniera diversa data la minore importanza del dato nei seguenti modi: chiusi a chiave in cassettiera per garantire la **riservatezza**, per la **disponibilità** del dato o scansione informatica (con relativa pseudonimizzazione ma in questo caso basterebbe la trasformazione in digitale) o copie da conservare in altra cassettiera, l'**integrità** del dato sarebbe garantita dalla chiusura a chiave.