Ordine degli Ingegneri della Provincia di Roma

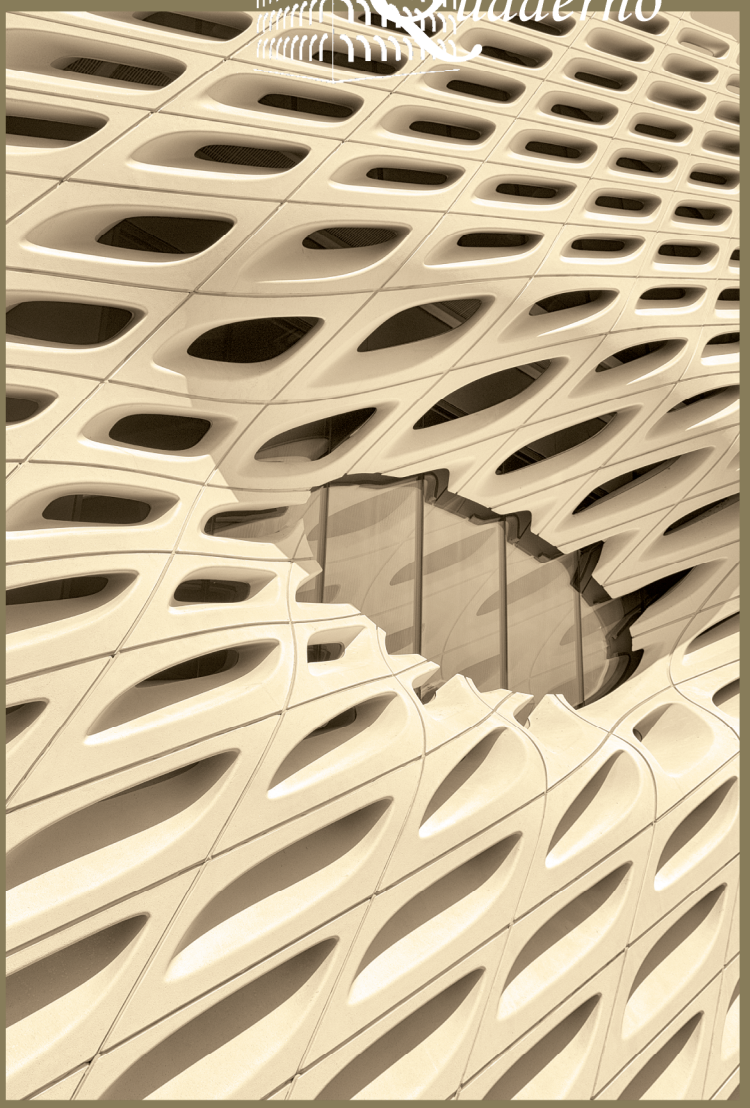
N 1S/2021

io roma

Quaderno

La Sicurezza Informatica per la protezione dei dati

Quaderno



In copertina:
Immagine di repertorio

DIGITAL UNIVERSE
DIGITAL UNIVERSE

Il saluto del Presidente

Dott. Ing. Carla Cappiello

La sicurezza informatica

La minaccia di cyber attacchi diventa sempre più reale con il crescere della digitalizzazione. Si presume che nel 2030 tale pericolo possa pesare circa l'1,2% del PIL mondiale. L'Italia a livello di competenze digitali possedute da cittadini e imprese si classifica al 25esimo posto in Unione Europea. Questo di certo non è un buon risultato.

Gli ormai numerosi fatti di cronaca legati alla violazione dei sistemi informatici pongono all'opinione pubblica molti quesiti sul tema della tutela della sicurezza dei dati dei cittadini, delle imprese e dei Governi. Non è più prevedibile se la minaccia cibernetica colpirà su larga scala infrastrutture critiche e grandi aziende o famiglie e aziende di piccole dimensioni. Una sola cosa è certa: il rischio di attacchi è destinato a aumentare, perché la digitalizzazione dei processi civili, sociali ed economici proseguirà tramite le tecnologie IoT (Internet of Things) e quelle di comunicazione mobile ultra-veloce (5G), ampliando la superficie d'impatto di azioni criminali intraprese e sfruttando le interconnessioni. Il numero di dispositivi elettronici connessi in tutto il mondo a internet supererà i 40 miliardi entro il 2023, raddoppiando i 20 miliardi attuali.

Gli obiettivi degli attacchi sono principalmente due: compromettere la funzionalità di infrastrutture informatiche per provocare danni o testare la solidità dei sistemi di difesa; spiare, raccogliere e trasmettere informazioni riservate, senza autorizzazione per recepire segreti industriali, informazioni sensibili per la sicurezza nazionale. Gli hacker, di qualunque natura o estrazione siano, si affidano sempre più a malware, cioè a programmi che vengono inseriti in un sistema informatico con l'obiettivo di compromettere la riservatezza, l'integrità o la disponibilità stessa dei dati.

La prima contromisura da adottare in un processo di miglioramento delle conoscenze di imprese e cittadini sarebbe la formazione trasversale, tra l'ingegneria e il diritto, da intendere come strumento necessario per evitare almeno gli attacchi più banali.
Con il Regolamento europeo 2016/679 sulla protezione dei dati personali (GDPR), si è data una grande attenzione alla sicurezza informatica, ponendo particolare focus alle attività degli stessi utenti che devono rimanere sempre all'interno di limiti preventivati e prevedibili.
Le informazioni sono il patrimonio principale di imprese, organizzazioni e singoli individui. Per questo la loro gestione deve rappresentare una priorità da difendere sia con norme specifiche sia con sistemi ingegneristici di alto livello.

Ing. Carla Cappiello
Presidente
Ordine degli Ingegneri della Provincia di Roma

L'Editoriale

Ing. Francesco Marinuzzi Ph.D.

Per uno sviluppo oltre che una protezione dell'economia dei dati

Quando entrai come consigliere all'Ordine, nel 2013 c'era una unica commissione ICT per tutto il terzo settore o settore dell'ingegneria dell'informazione. Una realtà che ben conoscevo perché anni prima ero stato segretario, vicepresidente e presidente di quella commissione.
Notai subito che le altre due aree dell'ingegneria, quella edile e quella industriale, avevano una fitta articolazione e che il tema della sicurezza era fondamentale: sicurezza nel lavoro, nei cantieri, etc.
Mi fu pertanto naturale pensare di istituire subito una commissione specifica di Sicurezza Informatica per la cui Presidenza, fin dal suo inizio, concordemente con tutto il Consiglio, segnalai la collega Paola Rocco. Una scommessa e una sfida, a distanza di tempo vinta che anche questa Speciale Pubblicazione testimonia.
Negli ultimi 8 anni la rilevanza e criticità della sicurezza digitale è aumentata a dismisura e con il famoso GDPR entrato in vigore nel 2018, la questione ha finito di comprendere tematiche, obblighi e questioni e informative e normative che van oltre a quelle strettamente connesse alla sicurezza informatica. Ottima, pertanto, la sinergia sottesa a questa pubblicazione con gli avvocati.
Sul tema della sicurezza informatica ho una mia posizione molto netta, opinabile ma comunque figlia della mia esperienza più che trentennale nel settore digitale.
La rivoluzione digitale è iniziata nel 1968, in una terra e in un clima di rottura e di piena libertà dei costumi contro le guerre, le regole e le istituzioni, in una cultura hippie del tutto estranea alla sicurezza. Ne stiamo pagando ancora le conseguenze, ad esempio, quando usiamo l'email, nata in quei tempi, e veniamo violati da allegati infetti o messaggi di phishing. Lo stesso schema di protezione delle user e password ha profondi limiti e la "doppia autenticazione" via cellulare, in alcuni casi ha permesso lo svuotamento di alcuni conti bancari con la tecnica dello Swap SIM. C'è bisogno di un profondo ripensamento delle architetture, delle soluzioni e dei processi associati che può anche portare a nuove forme rivoluzionarie del valore basate sul nuovo concetto di unicità digitale: in quest'ottica il boom dei ledger o database distribuiti, fra cui le "blockchain", lo sviluppo e la crescita delle cryptovalute e degli NFT in campo artistico, degli smartcontract oppure degli acquisti di nuova terra digitale quale, ad esempio, l'OVRLand, sono tutti fattori che indicano con forza la nuova direzione e le grandi opportunità associate che si offrono ora a chi le sa distinguere e cogliere. Sicuramente, allo stato attuale

dei processi, della cultura e delle soluzioni della PA, digitalizzarla massicciamente, magari grazie al Recovery Fund, senza introdurre e/o tenere in conto queste nuove dimensioni, rischia di essere un vero boomerang.

A questo scenario si aggiunge una cultura tutta europea dei dati come elementi da proteggere piuttosto che da valorizzare e da riconoscere nel loro valore verso i veri proprietari che sono gli utenti stessi che li producono in ogni istante. Probabilmente, rispetto agli USA, qui pesano ancora gli usi massicci di dati, con sistemi a schede perforate, che, secondo un famoso libro del giornalista investigativo Edwin Black, furono fatti nel primo Novecento per censire e poi perseguire la popolazione ebraica. Abbiamo cosi, qui in Europa, uno scenario schizofrenico dove da un lato ogni professionista, azienda e operatore economico è soggetto ad adempimenti e sanzioni molto forti e significative, fino al 4% del fatturato, nella gestione dei dati personali di ogni cliente e dall'altro i nativi digitali, spesso i figlio dei primi, danno e condividono in modo compulsivo continuamente dati, informazioni emozioni personali, foto, video senza alcun controllo, spesso anche all'insaputa dei propri genitori o tutori arricchendo a dismisura il potere informativo e dunque economico dei grandi Imperi Digitali made in USA.

Ci si augura, che dopo questa fase di Protezione GDPR, ne inizi subito una di GDDR dove alla P di Protezione venga sostituito la D di Development e sviluppo del valore dei dati. Questa nuova legislazione è fondamentale soprattutto ora per informare e dare un fattore moltiplicativo ai prossimi cospicui investimenti previsti e soprattutto fermare l'emorragia di valore verso l'estero in atto a livello di tutto il continente europeo.

Nel frattempo, cerchiamo comunque di minimizzare i rischi aggiuntivi e normativi e cogliamo l'opportunità del GDPR come momento di riflessione e miglioramento anche della sicurezza informatica esistente nelle nostre realtà operative. Le linee guida che qui pubblichiamo e i validi contributi sono preziosi elementi per questo percorso da affiancare a momenti formativi e di aggiornamento professionale che son sicuro le varie commissioni, ognuna per il suo ambito, non mancheranno di produrre in linea con i tanti eventi già fatti in tal senso.

Francesco Marinuzzi, Ph.D.
Direttore Editoriale

Relazione Introduttiva

Ing. Paola Rocco

Il presente numero è stato ideato a seguito dell'entrata in vigore del Regolamento Generale sulla Protezione dei Dati personali n. 2016/679 (General Data Protection Regulation o GDPR) per sensibilizzare e guidare l'ingegnere che opera quale professionista autonomo a rivedere il proprio approccio alla gestione dei dati personali, valutandone il trattamento secondo i principi fondamentali del regolamento, verificando le modalità e le finalità per cui vengono trattati, analizzando gli eventuali rischi connessi e fornendo un supporto per l'adozione delle soluzioni di sicurezza adeguate.

Al giorno d'oggi i nuovi modelli di sviluppo e le nuove tecnologie aumentano il patrimonio informativo delle imprese rendendo sempre più digitali i processi di business critici.

Il nuovo Regolamento Europeo in materia di protezione dei dati, il GDPR (General Data Protection Regulation), stabilisce norme relative alla tutela delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati, tutelando i diritti e le libertà fondamentali delle persone fisiche.

La sicurezza informatica, nella declinazione nella cybersecurity sta diventando oggi giorno materia di numerosi Master e anche di prime Lauree Magistrali in diverse Università ed è più che mai materia di interesse e competenza dell'Ingegnere al pari della Sicurezza sui luoghi sul lavoro, in quanto regolamenta la sicurezza dell'identità digitale delle persone e la protezione delle infrastrutture critiche e dei sistemi di controllo industriale.

All'interno del numero oltre alla Linea Guida all'applicazione del Regolamento UE 679/2016 per gli Ingegneri liberi professionisti e studi professionali di Ingegneria, sono presenti diversi articoli sul tema della protezione dei dati, che forniscono dei chiarimenti in merito agli strumenti utilizzati per la prevenzione contenimento e gestione dei possibili Data Breach, lo stato di avanzamento della direttiva ePrivacy e le sue relazioni con il GDPR, la DPIA.

L'invito rivolto a tutti i colleghi è quello di affrontare il Regolamento cogliendone, in primis, lo spirito e l'opportunità di mettere a fuoco la gestione dei dati personali nei propri processi operativi, rendendoli più efficaci e soprattutto più sicuri, a vantaggio del proprio business, ma anche a tutela dei diritti e delle libertà degli interessati.
Infine, un sentito ringraziamento a tutti i colleghi che hanno partecipato alla redazione della Linea Guida insieme con la Commissione Informatica, ai colleghi della Commissione Sicurezza Informatica che hanno contribuito con i loro articoli al numero e all'Ordine degli Avvocati e alla Commissione Privacy che ha contribuito a rileggere e validare gli aspetti giuridici contenuti nel documento, con cui abbiamo svolto anche diversi seminari sul tema.

Ing. Paola Rocco
Presidente Commissione Sicurezza

+/-
ON
AC

DPR
25 MAY 2018

Quaderno

Direttore responsabile
Stefano Giovenali

Direttore editoriale
Francesco Marinuzzi

Comitato di redazione

Sezione A
Carla Cappiello
Gioacchino Giomi
Lucia Coticoni
Giuseppe Carluccio
Carlo Fascinelli
Lorenzo Quaresima
Manuel Casalboni
Filippo Cascone
Alessandro Caffarelli
Massimo Cerri
Francesco Fulvi
Tullio Russo

Sezione B
Giorgio Mancurti

Amministrazione e redazione
Piazza della Repubblica, 59 - 00185 Roma
Tel. 06 4879311 - Fax 06 487931223

P. M. Art director
Tiziana Primavera

Assistenza Editoriale
Chiara Notargiacomo
Flavio Cordari
Nicolò Notargiacomo

Stampa
Press Up

Ordine degli Ingegneri della Provincia di Roma
Piazza della Repubblica, 59 - 00185 Roma
www.ording.roma.it
segreteria@ording.roma.it
editoriale@ording.roma.it

Finito di stampare: maggio 2021

Il Quaderno IOROMA è una estensione alla rivista IOROMA

La Direzione rende noto che i contenuti, i pareri e le opinioni espresse negli articoli pubblicati rappresentano l'esclusivo pensiero degli autori, senza per questo aderire ad esse.
La Direzione declina ogni qualsiasi responsabilità derivante dalle affermazioni o dai contenuti forniti dagli autori, presenti nei suddetti articoli.

FSC
www.fsc.org
MISTO
Carta da fonti gestite in maniera responsabile
FSC® C109382

Sommario

GLI EDITORIALI

Il saluto del Presidente **01**
di Carla Cappiello

L'Editoriale **04**
di Francesco Marinuzzi

Relazione Introduttiva **06**
di Paola Rocco

GLI ARTICOLI

Linea Guida: gli Ingegneri e il GPDR **12**

Strumenti di prevenzione e protezione per implementare la GDPR compliance **72**
P. Rocco

La Direttiva ePrivacy e il rapporto con il GDPR **78**
N. Castelliti

Gestione delle violazioni dei dati personali (data breach), prevenzione e reazione **94**
A. Alessandroni

La DPIA-Data Protection Impact Assessment **102**
N. Castelliti

L'AREA WEB DEL QUADERNO E DELLA RIVISTA **112**

LINEA GUIDA
GLI INGEGNERI E IL GPDR

Guida all'applicazione del Regolamento UE 679/2016
per gli ingegneri liberi professionisti e
studi professionali di Ingegneria

a cura di
Dott. Alessandro Bruttini
Ing. Giancarlo Di Lieto
Ing. Luisa Franchina
Ing. Giovanna Garritano
Dott. Andrea Lucariello
Ing. Francesco Micillo
Ing. Andrea Praitano
Ing. Paolo Reale
Ing. Paola Rocco
Ing. Carmelo Ungaro
Ing. Giuseppe G. Zorzino

1. Introduzione

1.1 Premessa

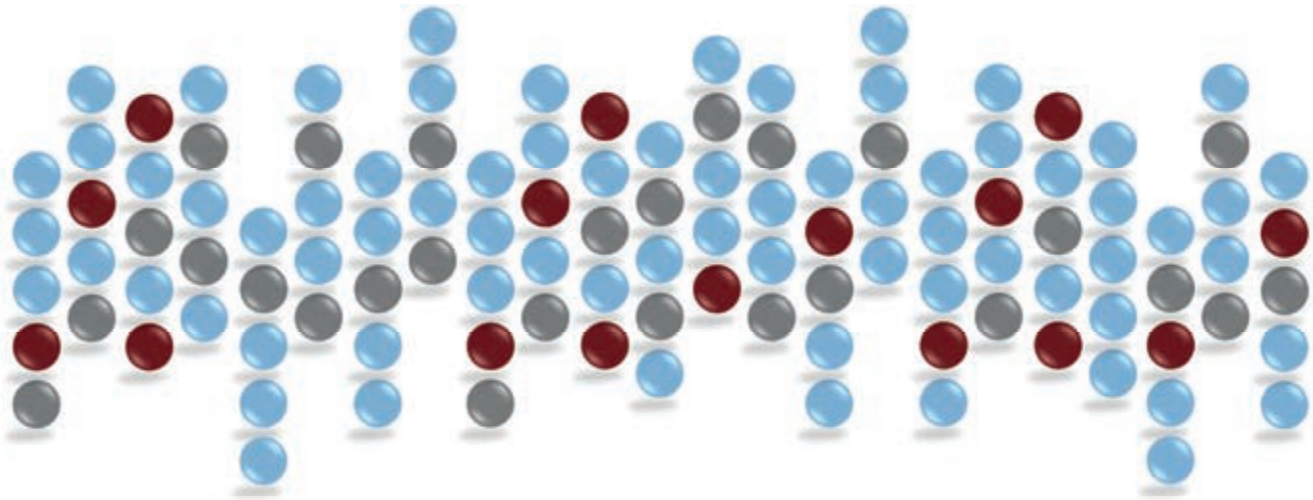
Il Regolamento Generale sulla Protezione dei Dati personali n. 2016/679 (General Data Protection Regulation o GDPR[1]), a partire dal 25 maggio 2018 è direttamente applicabile in tutti gli Stati membri. Il GDPR è stato Pubblicato sulla Gazzetta Ufficiale Europea il 4 maggio 2016 ed è entrato in vigore il 24 maggio 2016. La sua attuazione è stata posticipata di due anni al fine di dare la possibilità a tutte le organizzazioni ed ai professionisti di adeguarsi alle indicazioni della nuova normativa.

A distanza di oltre due anni dall'entrata in efficacia del GDPR il quadro normativo sulla protezione dei dati personali non è ancora completo ed aggiornato in tutte le sue parti[2]. Diverse organizzazioni hanno iniziato tardivamente i progetti di adeguamento per diverse ragioni, non ultimo il fatto che la normativa nazionale era ancora in corso di aggiornamento[3]. Alla data odierna il processo di adeguamento delle organizzazioni è in parte ancora in corso. Per questo motivo, sono ancora molte le categorie professionali, le Aziende e gli Enti che si interrogano su quali debbano essere, in concreto, gli adeguamenti necessari e quali rischi si corrono nel posticiparli.

In realtà, ad una lettura anche non particolarmente approfondita del testo del Regolamento, si potrebbe cogliere facilmente, insieme a molti altri aspetti, un tratto fondamentale di tale normativa che rappresenta più un'opportunità che non un vincolo oppressivo: il principio di "Responsabilizzazione"[4]. Con questo termine il legislatore europeo ha voluto assegnare al Titolare del Trattamento la libertà di scelta delle soluzioni tecniche ed organizzative che lui ritiene più idonee al fine di garantire il corretto Trattamento dei dati personali e la loro protezione. Il principio di Responsabilizzazione, così come altre parti della normativa, porta ad una "modularità" e contestualizzazione della normativa ai vari contesti in cui operano le organizzazioni che trattano i dati personali. Anche da qui nascono queste linee guida che vogliono andare ad aiutare ed indirizzare gli Ingegneri professionisti e gli studi professionali nella corretta applicazione del GDPR in ogni specifico contesto che li riguarda.

1.2 Obiettivo del documento

Questo documento vuole essere un'introduzione al GDPR ed alla normativa italiana a oggi vigente, con la finalità di fornire al professionista ingegnere una guida alla lettura ed interpretazione della normativa e delle linee di indirizzo nonché le buone pratiche per la sua implementazione. Non è da intendersi come sostitutivo del percorso di approfondimento della normativa europea e nazionale sulla protezione dei dati personali (partendo, ovviamente, dal GDPR), ma una sorta di ingresso facilitato al tema, senza pretesa di esaustività, con l'obiettivo di consentire un corretto inquadramento delle esigenze di categoria. Per tale ragione è stato strutturato in capitoli che sintetizzano il *quadro* normativo, una sezione relativa ai principali adempimenti[5], una sezione di FAQ nella quale trovare le risposte ai quesiti più ricorrenti sul tema, nonché degli esempi calati -ove possibile- in contesti realistici e, infine, dei modelli documentali di esempio per alcuni adempimenti che il professionista può prendere



come riferimento, adattandoli -ove necessario- al proprio contesto.
L'attuale stesura, orientata ad un obiettivo di semplificazione e di introduzione, potrà essere in seguito rivista sulla base dei feedback che verranno forniti dai colleghi.

1.3 Ambito di applicazione

Il presente documento si rivolge principalmente agli ingegneri liberi professionisti e agli studi associati costituiti da un limitato numero di professionisti, per quanto attiene alla gestione dei dati personali all'interno del proprio studio. Pertanto, il documento non intende essere di supporto alle specifiche attività di consulenza in ambito protezione dei dati personali[6] svolte dagli ingegneri liberi professionisti e dagli studi associati.
Non escludendo che alle presenti Linee Guida possano in seguito essere apportate ulteriori integrazioni ed estensioni, il criterio alla base della scelta dell'ambito è legato alla volontà e necessità di fornire attraverso una guida operativa, una prima risposta ai colleghi le cui esigenze di adeguamento al Regolamento Europeo sono – verosimilmente – ridotte come complessità e necessità di definizione del trattamento auspicabilmente utile alle proprie esigenze.
Il documento non ha la pretesa di rispondere a tutte le domande, bensì quella di fornire una "bussola" di orientamento in relazione alla domanda *"Cosa devo fare, nell'ambito della mia attività, per essere conforme al nuovo Regolamento Generale sulla Protezione dei Dati personali?"*.
Come già precedentemente accennato, è bene ricordare che queste Linee Guida non costituiscono un riferimento normativo sostitutivo del GDPR: per tale ragione – rimandando a questo per ogni approfondimento del caso – si declina ogni eventuale responsabilità in merito ad un uso di queste Linee Guida difforme dagli scopi per i quali sono state proposte.

Definizioni (ex art 4)

All'art. 4 del GDPR si trovano elencate le definizioni fondamentali della normativa, articolo al quale si rimanda per quanto attiene alle spiegazioni su: dato personale; trattamento; limitazione di trattamento; profilazione; pseudonimizzazione; archivio; titolare del trattamento; responsabile del trattamento; destinatario; terzo; consenso dell'interessato; violazione dei dati personali[7]; dati genetici; dati biometrici; dati relativi alla salute; stabilimento principale; rappresentante; impresa; gruppo imprenditoriale; norme vincolanti d'impresa; autorità di controllo; autorità di controllo interessata; trattamento transfrontaliero; obiezione pertinente e motivata; servizio della società dell'informazione; e organizzazione internazionale.

In questa sezione si vuole dare al lettore una chiave di lettura di alcune delle definizioni principali, viste nel contesto dell'ingegnere professionista o dello studio associato.
L'art. 1 del GDPR primo comma indica:

1. Il presente 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.

Il GDPR, così come la precedente Direttiva 46/95/CE che ha sostituito, ha una doppia finalità: la prima è quella di proteggere i dati personali delle persone fisiche (i cittadini che la norma chiama con il termine interessati[8]), la seconda è quella di consentire la libera circolazione degli stessi. Quindi, l'ambito a cui si applica questa normativa è costituito dai dati personali che sono definiti dall'art. 4 del GDPR come:

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;

Pertanto, sono dati personali tutte le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire riferimenti alle sue caratteristiche, abitudini, stile di vita, relazioni personali, stato di salute, situazione economica.
Non sono dati personali tutti quei dati che non sono relativi a persone fisiche o che non possono identificarli direttamente o indirettamente. In quest'ultima categoria possono ricadere anche i dati anonimizzati[9].

Nota: risulta essere un dato personale sia il nome Mario Bianchi insieme alle informazioni ad esso connesse quali, ad esempio, il suo codice fiscale (BNCMRA80A01H501R), la targa della sua automobile (AA 000 AA), il suo indirizzo email (***nome.cognome@provider.it***), ecc. Non risultano invece essere dati personali dati di entità giuridiche quali, ad esempio, Azienda S.p.A. o la sua partita IVA. Sono dati personali invece, quelli inerenti al legale rappresentante della persona giuridica o del personale di contatto all'interno della persona giuridica con cui si intrattengono rapporti.
Per l'ingegnere risulta fondamentale capire quali sono le informazioni trattate normalmente nell'attività lavorativa, quale è l'ambito di applicazione della normativa[10] e quali sono le misure

di sicurezza che si devono adottare.
Particolarmente importanti sono:

- i dati che permettono l'identificazione diretta - come i dati anagrafici (ad esempio: nome e cognome), le immagini, ecc. - e i dati che permettono l'identificazione indiretta, come un numero di identificazione (ad esempio, il codice fiscale, il numero di telefono, la targa di un'automobile)[11];
- i dati rientranti in particolari categorie: si tratta dei dati precedentemente definiti "sensibili" dal D.Lgs. 196/03, cioè quelli che rivelano l'origine razziale o etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza ad organizzazioni sindacali, relativi alla salute, alla vita o all'orientamento sessuale. Il GDPR (art. 9) ha specificatamente incluso nella nozione anche i dati genetici e i dati biometrici;
- i dati relativi a condanne penali e reati: si tratta dei dati c.d. "giudiziari", cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato.

Fondamentale è anche comprendere cosa si intende per trattamento di dati personali. Il GDPR (art. 4) definisce «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.
È importante ricordare che la normativa si applica al trattamento dei dati personali in qualsiasi forma, quindi è indifferente la modalità utilizzata, se elettronica e/o tramite supporto cartaceo.

1.4 Figure coinvolte

Gli attori coinvolti nei processi di tutela dei dati personali sono in parte "interni" all'organizzazione[12] che tratta i dati personali, e anche esterni. Le figure esterne sono:

- **Interessato**: è la persona fisica a cui si riferiscono i dati personali che sono trattati[13];
- **Garante della Protezione dei Dati Personali[14]:** è l'Autorità nazionale che ha il ruolo di garantire che le organizzazioni nazionali rispettino il diritto dei cittadini al trattamento dei dati personali. Esiste un'autorità per ognuno degli stati europei;
- **Comitato europeo per la protezione dei dati:** i compiti del Comitato sono definiti dall'art. 70 del GDPR;
- **Garante europeo della protezione dei dati[15]:** è il Supervisor che ha il ruolo di garantire che le istituzioni e gli organi dell'UE rispettino il diritto dei cittadini alla protezione dei propri dati personali.

Le figure principali coinvolte nel trattamento sono:

- **Titolare del Trattamento**: il Titolare del Trattamento (semplicemente Titolare) è la persona fisica, l'autorità pubblica, l'impresa, l'ente pubblico o privato, l'associazione, professionista, studio associato, ecc., che definisce le finalità e i mezzi del trattamento (art. 4, paragrafo 1, punto 7, del GDPR).
- **Responsabile del Trattamento**: il Responsabile del Trattamento (semplicemente Responsabile) è la persona fisica o giuridica esterna al Titolare al quale questo affida specifici e definiti compiti di gestione e controllo svolti per suo conto e sotto sue indicazioni (art. 4, paragrafo 1, punto 8, del GDPR). Il GDPR ha formalizzato che un Responsabile ha la possibilità, sotto autorizzazione specifica o generale del Titolare, di designare un altro soggetto c.d. "sub-responsabile" (art. 28, paragrafo 2 del GDPR).

L'ingegnere professionista o studio associato può ricadere nella figura del Titolare o del Responsabile o di entrambe (per trattamenti differenti). L'ingegnere sarà Titolare dei dati personali che raccoglie direttamente dai propri clienti (persone fisiche). L'ingegnere sarà Responsabile per le attività di trattamento su dati non raccolti direttamente dalle persone fisiche, che lui svolge sulla base di un contratto di erogazione di servizi professionali che implicano un trattamento dei dati personali.

- **Data Protection Officer (DPO)**: il Data Protection Officer, o anche **Responsabile della Protezione dei Dati (RPD)**, è la figura designata a sorvegliare l'osservanza del regolamento all'interno di una organizzazione, informare e fornire consulenza al Titolare o al Responsabile, cooperare e fungere da punto di contatto con l'Autorità di controllo[16]. Tale figura non deve essere formalizzata da tutte le organizzazioni, ma solo in casi specifici (si veda Art. 37 del GDPR).

Il GDPR (a differenza del D.Lgs. 196/03 pre-adeguamento al GDPR) non prevede espressamente la figura dell'incaricato, ma di fatto ne parla nell'articolo 29 relativo al "Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento". **L'incaricato** o **autorizzato** è la persona fisica che effettua materialmente le operazioni di trattamento sui dati personali sotto la diretta responsabilità del Titolare o del Responsabile. Tali figure sono denominate designate nell'art 2.quaterdecies del D.lgs. 101/2018.

Si citano a titolo informativo le figure professionali definite dalla norma UNI 11697:2017 ed associate alla protezione dei dati: "privacy manager", "specialista privacy" e "valutatore privacy". Queste figure possono essere di aiuto all'organizzazione o al professionista per quanto attiene la tematica della protezione dei dati personali. Si rimanda alla suddetta norma per la descrizione delle conoscenze, competenze e abilità associate a questi ruoli e le responsabilità che possono essere loro assegnate.

2. SINTESI DEI PRINCIPALI ADEMPIMENTI PER GLI INGEGNERI

In questa sezione si vuole fornire un aiuto agli ingegneri professionisti e agli studi associati nel

comprendere cosa deve essere fatto per essere conformi alla normativa. Aspetto importante è che qui viene data un'interpretazione nel contesto di uno studio tipo. Queste possono quindi essere solo delle indicazioni di tipo generale in quanto andrebbe compreso caso per caso cosa fare e quale soluzione è la migliore nel contesto specifico in cui opera lo specifico ingegnere professionista o studio associato.

2.1 Passi operativi da svolgere per la verifica degli adempimenti

Un possibile flusso logico che l'ingegnere professionista o lo studio associato può seguire è quello riportato nella figura 1.

1) **Identificazione dei trattamenti svolti**: in questa prima fase (vedi § 3.3) si devono andare a identificare i trattamenti di dati personali che sono svolti dall'ingegnere professionista o dallo studio associato. Possibili prodotti di questa fase possono essere:
   a. Registro delle Attività di Trattamento.
2) **Individuazione delle finalità e basi giuridiche del trattamento**: in questa fase (vedi § 3.4) si verifica che il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle condizioni riportate nell'articolo 6 del GDPR. Possibili prodotti di questa fase sono:
   a. Informative al trattamento;
   b. Modulo di consenso al trattamento;
   c. Richieste di conferma del consenso al trattamento per i dati già raccolti che sono trattati con finalità diverse a quel la per i quali sono stati raccolti. Questa modalità può essere altresì utilizzata per i dati raccolti di cui si è perso traccia della finalità di trattamento;
   d. Verifica delle Clausole contrattuali da utilizzare per eventuali trasferimenti extra UE (articolo 46 GDPR).
3) **Valutazione d'Impatto sulla protezione dei dati personali**: in questa fase (vedi § 3.6) viene svolta la così detta DPIA (Data Protection Impact Assessment) sui trattamenti che sono reputati rischiosi. Possibili prodotti di questo fase possono essere:
   a. Valutazione d'impatto sulla protezione dei dati personali per i nuovi trattamenti reputati critici;
   b. Misure di sicurezza organizzative aggiuntive da adottare sul nuovo trattamento;
   c. Misure di sicurezza tecniche aggiuntive da adottare sul nuovo trattamento;
   d. Richiesta di consultazione preventiva per i trattamenti che continuano ad essere critici anche a seguito delle misure di sicurezza tecniche ed organizzative aggiuntive.
4) **Protezione dei dati personali**: in questa fase (vedi § 3.5) vengono identificati i rischi connessi ai dati personali e le misure di sicurezza messe a loro protezione. Possibili prodotti di questo fase possono essere:

a. Analisi dei rischi;
b. Misure di sicurezza organizzative adottate;
c. Misure di sicurezza tecniche adottate;
d. Politica di Data Protection by Design e by Default.

5) **Identificazione e gestione delle violazioni dei dati personali**: questa fase (vedi § 3.8) ha obiettivi multipli: da un lato deve definire come vengono identificate le violazioni dei dati personali (in termini di violazioni di Riservatezza, Integrità e/o Disponibilità), dall'altro la gestione delle violazioni e valutazione interna fino alla notifica all'Autorità Garante per la Protezione dei Dati Personali e, se necessario, la comunicazione agli interessati. Possibili prodotti di questo fase possono essere:
   a. Procedura di escalation interna per la valutazione delle violazioni dei dati personali;
   b. Procedura di notifica all'Autorità Garante della Protezione dei Dati Personali;
   c. Procedura per la comunicazione agli interessati.

6) **Gestione dei diritti degli interessati**: questa fase ha l'obiettivo di definire il processo di gestione delle richieste di esercizio dei propri diritti da parte degli interessati. Possibili prodotti di questo fase possono essere:
   a. Processo/procedura da seguire a seguito di una richiesta di esercizio dei diritti da parte degli interessati.

2.2 Principi applicabili al trattamento di dati personali

I principi applicabili ai trattamenti sono indicati nel Capo II del GDPR, in particolare nell'art. 5. All'interno di questa sezione si vuole proporre una possibile interpretazione calata nel contesto della figura dell'ingegnere professionista o dello studio associato.

Principio di liceità, correttezza e trasparenza: deve essere garantito che i dati personali siano trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (art. 5.a del GDPR).

Principio di limitazione delle finalità: deve essere garantito che i dati sono raccolti (art. 5.b del GDPR) per finalità determinate, esplicite e legittime («**limitazione della finalità**»). Nel contesto specifico dell'ingegnere professionista o dello studio associato questo significa che i dati sono richiesti agli interessati e raccolti per una finalità specifica (ad es. lo svolgimento dell'attività professionale) ed utilizzati esclusivamente per questa finalità (ad es. non utilizzati per attività di marketing, senza preventivo consenso).

Consiglio: il trattamento dei dati personali è legittimato da una base giuridica (ne sono definite 6[21], come ad es. il consenso). Il professionista può predisporre un modulo per la raccolta dei consensi (vedi § 7.1). Il Consenso va richiesto in maniera granulare per ogni finalità perseguita, qualora non si possa individuare una differente base giuridica.

Principio di minimizzazione dei dati: i dati personali raccolti e trattati (art. 5.c del GDPR) devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («**minimizzazione dei dati**»).

Consiglio: aspetto importante che l'ingegnere professionista o lo studio associato deve tenere in considerazione è il non eccedere

1. L'Ingegnere libero professionista o lo studio associato rispetto al trattamento dei dati personali può ricoprire il ruolo di: a. Titolare del Trattamento per quanto riguarda il trattamento dei dati dei propri clienti (persone fisiche); b. Responsabile del Trattamento per quanto riguarda il trattamento dei dati per conto di un suo cliente (azienda o organizzazione) per il quale opera sulla base di specifici contratti[17]; c. Contitolare, allorché determina congiuntamente ad altro Titolare finalità e mezzi del trattamento[18]; d. Amministratore di sistema nell'ambito ICT;
2. Come Titolare del Trattamento, deve verificare che ci sia sempre una base di liceità del trattamento (vedi §3.2);
3. Come Titolare del Trattamento, deve verificare che i dati raccolti siano adeguati, pertinenti e limitati rispetto alla finalità del trattamento (vedi §3.2)[19];
4. Come Titolare del Trattamento, deve trattare i dati esclusivamente per le finalità per i quali sono stati raccolti (vedi §3.2) (le comunicazioni marketing richiedono il consenso);
5. Come Titolare del Trattamento, deve definire la durata della conservazione dei dati, compatibilmente con la legislazione in vigore (vedi §3.2);
6. Come Titolare del Trattamento, deve fornire l'informativa agli interessati e, quando previsto, raccogliere il consenso (vedi §3.4);
7. Come Titolare del Trattamento, deve applicare i principi di Data Protection by Design e by Default (vedi §3.7);
8. Come Titolare del Trattamento, ha l'obbligo di contrattualizzare la contitolarità se presente (art. 26 del GDPR);
9. Come Titolare del Trattamento, documenta qualsiasi violazione dei dati personali (vedi §3.8);
10. Come Titolare del Trattamento, ha l'obbligo di cooperazione con le Autorità di Controllo;
11. Sia come Titolare che come Responsabile, deve in casi particolari mantenere un Registro delle attività di trattamento, anche se nella pratica è una buona norma redigerlo e aggiornarlo sempre. Il Registro infatti costituisce il primo passo da effettuare per censire tutte le attività di trattamento (vedi §3.3). Si raccomanda pertanto di tenere sempre un registro aggiornato. Il regolamento specifica comunque che l'obbligo del registro non vige per le organizzazioni con meno di 250 dipendenti, a meno che il trattamento non includa un rischio per i diritti e le libertà delle persone interessate, non occasionale o se si riferisce in particolare a dati sensibili o a dati relativi a condanne e reati[20].
12. Valutare i rischi del trattamento e l'Attuazione di misure tecniche organizzative adeguate (vedi §3.5 e §3.6);
13. Deve trattare i dati personali in maniera da garantire un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (vedi §3.5);

14. Fare in modo che le persone coinvolte (colleghi, collaboratori, tirocinanti) siano adeguatamente informati e coinvolte nel processo di protezione dei dati personali;
15. Come Titolare del Trattamento deve provvedere alla nomina formale di eventuali organizzazioni esterne in qualità di Responsabile del Trattamento e deve comunicare loro le misure di sicurezza da adottare a protezione dei dati personali da loro trattati per suo conto;
16. È tenuto ad un riesame periodico e all'aggiornamento delle misure di sicurezza (vedi §3.5).
17. Come Responsabile del Trattamento deve seguire le indicazioni fornitegli dal Titolare del Trattamento per quanto attiene la protezione dei dati personali trattati per suo conto;
18. Come Responsabile del Trattamento deve segnalare al Titolare del Trattamento eventuali violazione dei dati personali intercorsi sui dati personali trattati per suo conto.

con i dati raccolti, che devono essere coerenti con le finalità. Ad es. non dovrebbero essere richiesti/raccolti dati non strettamente necessari per la finalità prevista al momento della richiesta, nella mera ipotesi che "non si sa mai, potrebbero servire".

Principio di esattezza:
i dati raccolti devono essere esatti e aggiornati (art. 5.d del GDPR). Devono essere adottate tutte le misure ragionevoli per rettificare o cancellare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («**esattezza**»).

Consiglio: bisogna tenere in considerazione che il travaso di dati da un formato ad un altro (ad es. da un modulo cartaceo ad un archivio informatizzato) è potenzialmente foriero di errori. Ove possibile, è opportuno predisporre sistemi che permettano direttamente all'interessato l'inserimento dei dati e/o, se necessario, la verifica ed aggiornamento degli stessi, ad es. attraverso la predisposizione di moduli web[22].

Principio di limitazione della conservazione:
i dati personali raccolti non possono essere conservati per un periodo di tempo indefinito (art. 5.e del GDPR), ma il tempo di conservazione deve essere coerente con le finalità del trattamento. 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, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal GDPR a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»).

Consiglio: alla conservazione dei dati personali concorrono diversi aspetti, il primo è la finalità con cui sono raccolti insieme alla data di acquisizione; i tempi vengono azzerati ad ogni nuova raccolta o motivazione (ad es. la raccolta dei dati di un cliente al fine di svolgimento di un'attività professionale ripartono ad ogni richiesta -e raccolta o aggiornamento- dei dati stessi per lo svolgimento della prestazione). Altri aspetti

Figura 1

sono costituiti da vincoli normativi quali, ad es., la conservazione dei dati connessi alla fatturazione della prestazione professionale. Nell'informativa bisogna indicare il tempo di conservazione o almeno i criteri con sui si determina il periodo di conservazione. Non esiste un tempo standard di conservazione, ma dipende [23].

Principio di sicurezza dei dati personali:
i dati personali raccolti devono essere trattati in modo tale che sia garantito un appropriato livello di sicurezza attraverso l'adozione di misure tecniche e organizzative adeguate, preservandoli da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale (**«integrità e riservatezza»**).

Nota: il principio riportato all'art. 5.f del GDPR indica l'integrità e la riservatezza mentre l'art. 32 "Sicurezza del Trattamento" estende il concetto di sicurezza nella sua accezione più ampia di Riservatezza, Integrità, Disponibilità e Resilienza.

2.3 Registro delle attività di trattamento

L'art. 30 del GDPR istituisce l'obbligo, nel contesto del principio di responsabilizzazione e a meno che non si ricada nelle eccezioni, di tenere un registro delle attività di trattamento da parte del Titolare del Trattamento o del Responsabile del Trattamento. Il Registro deve essere mantenuto in forma scritta e può essere anche in formato elettronico. La norma non definisce un modello puntuale del registro, ma indica le informazioni minime che deve contenere (art. 30 comma 1 del GDPR):

a) il nome e i dati di contatto del Titolare del trattamento e di ogni contitolare del trattamento, del rappresentante del Titolare del trattamento e del Responsabile della Protezione dei dati (se designato);
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;
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.

Analogo obbligo sussiste per il Responsabile del trattamento, il quale deve tenere un registro di tutte le attività di trattamento dei dati personali svolte per conto di un titolare, contenente:

a) nome e 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 dell'eventuale 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 ed organizzative.

Il contenuto minimo del registro è costituito dai campi sopra elencati, tuttavia, nulla vieta a un Titolare o Responsabile di inserire ulteriori informazioni se lo riterrà opportuno nell'ottica della complessiva valutazione di impatto dei trattamenti svolti (vedi §3.6). Su richiesta, il Titolare o il Responsabile mettono il registro a disposizione dell'Autorità Garante della Protezione dei Dati Personali in caso di ispezioni.
Nonostante la non obbligatorietà del Registro -salvo i casi già citati previsti dall'art. 30- il Garante della Protezione dei Dati Personali, sin dalle prime linee guida sull'applicazione del Regolamento ha precisato che la tenuta del Registro dei trattamenti non costituisce un adempimento meramente formale bensì è parte integrante di un sistema di corretta gestione dei dati personali. Pertanto, ha invitato tutte le organizzazioni a predisporre il Registro e a compiere comunque una ricognizione generale dei trattamenti effettuati e delle rispettive caratteristiche per un corretto processo di adeguamento alla normativa, indipendentemente dalla dimensione dell'organizzazione stessa e dai requisiti di esenzione.
Possiamo qui aggiungere che la formalizzazione del Registro delle Attività di Trattamento è un primo passo per l'organizzazione per capire quali dati tratta, su quali sistemi e/o applicativi avviene il trattamento, per quali finalità e chi è coinvolto nel trattamento. Senza queste informazioni risulterebbe complesso definire le finalità di trattamento per cui i dati sono raccolti. Pertanto, è opportuno che tutte le organizzazioni e anche da parte dell'ingegnere professionista o

dello studio associato, sia sempre formalizzato il Registro, anche se in modalità semplificata.

Nota: il GDPR indica che il Registro delle Attività di trattamento non deve essere obbligatoriamente tenuto per le organizzazioni che hanno meno di 250 dipendenti tranne nel caso sussistano determinati trattamenti più pericolosi.

Nell'appendice § 7.4 si riporta un template che l'ingegnere professionista o lo studio associato può adottare e adattare per la tenuta del proprio Registro delle Attività di Trattamento.

2.4 Informativa e consenso

La normativa consente il trattamento dei dati personali da parte di qualsiasi organizzazione a condizione che:

- sia presente una base giuridica che consente il trattamento;
- i dati siano adeguatamente protetti.

Le possibili basi giuridiche previste per un legittimo trattamento sono:

1) Consenso;
2) Adempimento di obblighi contrattuali;
3) Obblighi di legge cui è soggetto il titolare del trattamento;
4) Interessi vitali della persona interessata o di terzi;
5) Legittimo interesse prevalente del titolare o di terzi cui i dati vengono comunicati;
6) Interesse pubblico o esercizio di pubblici poteri (non applicabile per le autorità pubbliche).

Indipendentemente dalla base giuridica del trattamento l'organizzazione deve fornire adeguata informativa all'interessato. Pertanto, affinché il trattamento che si intende porre in essere sia lecito e trasparente, il Titolare deve rendere adeguata informativa all'interessato ai sensi degli artt. 13 e 14 del GDPR. L'informativa è dovuta sia nel caso in cui la raccolta avvenga direttamente presso l'interessato stesso (art. 13) e va presentata contestualmente, sia che i dati vengano raccolti da terze parti (art. 14) nel qual caso deve essere fornita entro un termine ragionevole, ma al più tardi entro un mese.

Il GDPR indica puntualmente il contenuto dell'informativa, specificando che le informazioni debbano essere presentate con un linguaggio chiaro, comprensibile e adeguato allo scopo ed al destinatario a cui queste sono destinate. Le informazioni che devono essere fornite sono:

a) identità e dati di contatto del Titolare del trattamento e, ove applicabile, del suo rappresentante;
b) dati di contatto del Responsabile della protezione dei dati (DPO), ove applicabile;
c) finalità e base giuridica del trattamento;
d) legittimi interessi perseguiti dal Titolare del trattamento o da un terzo qualora la base giuridica del trattamento sia costituita da legittimi interessi;
e) categorie di dati personali interessati (necessario ex art. 14, nell'informativa ex art. 13 va comunque indicato quali dati si raccolgono e come si trattano);
f) destinatari (o categorie di destinatari) dei dati personali;
g) informazioni sui trasferimenti a paesi terzi, fatto stesso del trasferimento e informazioni

sulle garanzie applicabili (compresa la presenza o l'assenza di una decisione di adeguatezza della Commissione) e strumenti per ottenerne copia o per sapere dove sono disponibili;

h) periodo di conservazione (o, se non disponibile, criteri per determinarlo);
i) diritti dell'interessato relativamente a: accesso; rettifica; cancellazione; limitazione del trattamento; opposizione al trattamento; portabilità;
j) diritto di revocare il consenso in qualsiasi momento nei casi in cui il trattamento lo presuppone (in forma esplicita o attraverso un'azione inequivocabile);
k) diritto di presentare un reclamo all'autorità di controllo;
l) precisazione del fatto che esista o no un obbligo previsto per legge o per contratto di fornire le informazioni o se sia necessario stipulare un contratto o se sussista l'obbligo di comunicare le informazioni, e le possibili conseguenze dell'omissione (necessario solo ex art. 13);
m) fonte da cui originano i dati personali e, se applicabile, se si tratta di fonte accessibile pubblicamente (necessario solo ex art. 14);
n) esistenza di un processo decisionale automatizzato, profilazione inclusa e, se del caso, informazioni pregnanti circa la logica seguita e l'importanza e le conseguenze previste del trattamento per gli interessati.

Nota: analizzando tale elenco si può notare che l'informativa deve essere fornita all'interessato dal Titolare; infatti, qualora si compiano attività di trattamento in qualità di Responsabile non si è tenuti all'obbligo di informativa in quanto il trattamento è svolto per conto e su indicazione del Titolare che l'ha precedentemente fornita.

Nell'appendice § 7.2 si riporta un template che l'ingegnere professionista o lo studio associato possono adottare ed adattare per il consenso e le informative.

Consiglio: qualora debbano essere raccolti i medesimi dati per finalità multiple e la base giuridica delle stesse è il consenso, si può predisporre un unico modulo di raccolta che riporta le diverse finalità di trattamento e i consensi separati per singola finalità.

Dove la base giuridica è il consenso questo non può essere fornito "per silenzio assenso" cioè deve essere richiesto il consenso esplicito[24].

Qualora si dovesse procedere ad un trattamento per finalità ulteriori, rispetto a quelle per cui detti dati sono stati raccolti, è fatto obbligo in capo al titolare del trattamento fornire all'interessato le informazioni relative a questo nuovo trattamento e, ove necessario, richiedere il consenso.

Il consenso deve essere fornito in modo libero non necessariamente in forma scritta, è però importante ricordare che è responsabilità del Titolare dimostrare che l'interessato ha fornito il consenso. La forma documentata (ad es. scritta, tramite flag o la registrazione) può essere necessaria al fine della dimostrazione di aver acquisito il consenso.

2.5 Trattamento di categorie particolari di dati personali

Quando si fa riferimento a dati personali "particolari" si intendono:

- dati personali che permettono di identificare l'origine razziale o etnica dell'interessato;
- dati personali che rilevano opinioni politiche;
- dati personali che fanno riferimento alle convinzioni religiose o filosofiche;
- dati personali che permettono di verificare l'appartenenza dell'interessato a un gruppo sindacale;
- dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica;
- dati relativi alla salute, dati relativi alla vita sessuale o all'orientamento sessuale della persona.

Sulla base di quanto espresso nel considerando n. 51, le categorie particolari di dati personali necessitano di livelli di protezione "maggiori" poiché questi sono dati personali, per loro natura, particolarmente critici sotto il profilo dei diritti e delle libertà fondamentali, dal momento che dal loro trattamento potrebbero derivare dei rischi significativi per i diritti e per le libertà fondamentali dei soggetti interessati. Pertanto, è consigliabile trattare dati personali particolari solo nel caso in cui l'interessato abbia prestato il proprio consenso esplicito al trattamento, salvo che tali dati non siano intrinsecamente necessari per lo svolgimento delle attività professionali.

Infatti, sono presenti delle fattispecie che rendono lecito il trattamento dei dati particolari anche quando l'interessato non abbia prestato il suo consenso.

Tra queste vi sono:

1. Il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro. Ad esempio: non è necessario richiedere il consenso per trattare i dati relativi assenze per malattia, certificati e visite mediche, documentazione relativa alla gravidanza, ecc.
2. Il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso. Ad esempio: è lecito trattare informazioni relative allo stato di salute a fini di soccorso immediato di un

infortunato, anche se l'infortunato è nell'impossibilità di prestare il proprio consenso.

3. Il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato. Ad esempio: dati pubblicati spontaneamente dall'interessato e accessibili al pubblico.
4. Il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro. I dati devono essere trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale. Ad esempio: non è necessario richiedere il consenso per valutazione dell'idoneità alla mansione lavorativa e finalità connesse.

2.6 Sicurezza del trattamento e analisi del rischio art. 32

Il GDPR stabilisce, all'art. 32, il dovere per il Titolare e per il Responsabile di adottare misure organizzative e tecniche adeguate a garantire la sicurezza del trattamento, tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche. Pertanto, la sicurezza dei dati personali deve essere commisurata al rischio per gli interessati, questo significa che non tutti i dati personali devono essere protetti allo stesso modo.

Il Titolare deve valutare i rischi inerenti al trattamento e attuare misure a protezione finalizzate a ridurre tali rischi, assicurando un adeguato livello di sicurezza che impedisca la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale.

Il GDPR individua alcune misure di sicurezza che possono essere adottate tra cui la pseudonimizzazione e la cifratura dei dati personali.

Le misure di sicurezza tecniche ed organizzative che vengono identificate devono essere in grado di garantire, nel complesso, la Disponibilità, l'Autenticità, l'Integrità, la Riservatezza e la Resilienza dei dati personali degli interessati.

Per Riservatezza si intende la caratteristica per la quale l'accesso alle informazioni è limitato a un gruppo preventivamente definito ed autorizzato a questo.

Tra le misure di sicurezza che possono essere adottate per poter garantire la riservatezza dei dati personali all'interno di uno studio di un ingegnere professionista o di uno studio associato vi sono[25]:

- Protezione dell'uso del computer da misure atte a garantire la riservatezza delle informazioni. Esempi:
  - L'accesso ai computer ed alle applicazioni deve essere protetto attraverso credenziali di autenticazione (nome utente e password);
  - La password deve essere sufficientemente robusta (almeno 8 caratteri alfa numerici e speciali) e deve essere rinnovata periodicamente;
  - La cifratura del disco rigido del computer portatile dell'ufficio;
  - La cancellazione sicura del disco prima della dismissione/rottamazione/vendita/cessione;
  - L'aggiornamento periodico del sistema operativo;
  - L'aggiornamento periodico degli applicativi;
  - Ecc..
- Protezione della documentazione cartacea con misure atte a garantire la riservatezza delle informazioni. Esempi:
  - Chiusura della documentazione cartacea contenente dati personali in armadi chiusi a chiave;
  - Distruzione della documentazione cartacea attraverso distruggi-documenti;
  - Ecc.
- Protezione delle comunicazioni. Esempi:
  - Discussione di informazioni o comunicazione di dati personali in luoghi privati;
  - Utilizzo di sistemi di posta elettronica di tipo "business";
  - Invio di documentazione via mail cifrata (ad es. attraverso un file zip protetto da password);
  - Ecc.
- Protezione della rete interna all'ufficio. Esempi:
  - Firewall perimetrale a protezione dell'accesso esterno;
  - Sostituzione delle password e delle utenze di default sui sistemi di rete;
  - Utilizzo di reti WiFi con password e sistema di cifratura;
  - Utilizzo di reti WiFi con SSID nascosto;
  - Impostazione di una rete WiFi "Ospiti";
  - Ecc.

Per Integrità si intende il grado con cui le informazioni sono identiche al dato originale, prive di errori (sia intenzionali che accidentali) ed aggiornate. L'Integrità è infatti caratterizzata da due aspetti: correttezza e completezza delle informazioni.

Alcune possibili misure di sicurezza che possono essere prese per poter garantire l'integrità dei dati personali all'interno di uno studio di un ingegnere professionista o di uno studio associato sono:

- Verifica inserimento dei dati:

GENERAL DATA PROTECTION

- I sistemi sono predisposti con controlli di correttezza dell'inserimento dei dati (ad es. verifica formato per l'inserimento del Codice Fiscale);
- I sistemi hanno meccanismi di inserimento guidati (ad es. per una data);
- Riduzione al minimo del travaso di dati manuale;
- Ecc.

• Registrazione degli accessi e delle attività:
- Gli accessi alle risorse informatiche sono registrati in file di log;
- Le attività svolte localmente sulle postazioni di lavoro sono registrate in file di log;
- I file di log sono salvati in un repository centralizzato con accesso controllato;
- Ecc.

• Installazione del software:
- I software sono installati da utenti amministrativi con privilegi superiori rispetto a quelli dell'utente utilizzatore del computer;
- I computer devono essere dotati di un antivirus costantemente aggiornato, possibilmente con funzionalità di personal firewall;

• Controllo trasferimento dei file:
- Il trasferimento di informazioni fra sistemi diversi include verifica dell'integrità di quanto trasmesso ad es. attraverso la verifica dell'hash del file;
- Comparazione dei file inviati rispetto al file origine.

Per Disponibilità si intende il grado in cui le informazioni sono disponibili all'utente e/o al sistema informativo nel momento in cui queste vengono richieste. La Disponibilità è caratterizzata da tre aspetti e sono:

- temporale - i sistemi informativi sono disponibili quando necessario;
- continuità - il personale può continuare a lavorare in caso di guasto;
- robustezza - vi è una capacità sufficiente per consentire a tutto il personale nel sistema di lavorare.

Possibili misure di sicurezza che possono essere prese per poter garantire la disponibilità dei dati personali all'interno di uno studio di un ingegnere professionista o di uno studio associato sono:

- Sicurezza dei dischi dei sistemi server:
  - Utilizzo di sistemi server con dischi in RAID (1 o 5);
  - Utilizzo di sistemi SAN/NAS di archiviazioni di rete con dischi in RAID (1 o 5);
- Backup delle postazioni di lavoro:
  - Utilizzo di sistemi di backup automatizzato o manuale per copie di ripristino dei dati;
  - Utilizzo di repository in cloud per la conservazione delle copie;
- Continuità operativa:
  - Accordi con studi professionali per ospitarsi in casi di inagibilità dello studio.

Per Resilienza si intende la capacità intrinseca di un sistema di modificare il proprio funzionamento prima, durante e in seguito ad un cambiamento improvviso o ad una perturbazione, in modo da poter continuare le operazioni necessarie sia in condizioni previste che in condizioni impreviste.

Infine, chiunque agisca sotto l'autorità di un Titolare o Responsabile non può trattare i dati personali se non è istruito in tal senso da questi. Pertanto, il libero professionista (o lo studio professionale) che svolge trattamenti per conto di un Titolare (o di un Responsabile) dovrà necessariamente essere istruito in merito alle misure di sicurezza da adottare e potrebbe essere eventualmente soggetto a verifiche ispettive intese a valutare il grado di recepimento delle istruzioni che ha ricevuto.

2.7 Valutazione d'impatto sulla protezione dei dati personali (artt. 35-36)

La valutazione d'impatto sulla protezione dei dati (DPIA – Data Protection Impact Assessment[26]) è una sorta di analisi dei rischi che va svolta prima di procedere ad un trattamento che comporti un impatto sugli interessati. È uno strumento importante per la responsabilizzazione in quanto sostiene il Titolare nel garantire e dimostrare la conformità al GDPR.

In linea con l'approccio basato sul rischio adottato dal Regolamento, non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento, ma soltanto quando questo, *"considerati la natura, l'oggetto, il contesto e le finalità, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche"*.

I trattamenti che devono essere sottoposti a valutazione preventiva d'impatto sono raggruppabili in 9 categorie che sono state recentemente ampliate dal Garante della Protezione dei Dati Personali con il provvedimento di ottobre del 2018 (provvedimento 467)[27]. Di seguito si riportano le casistiche previste dall'Allegato 1 al Provvedimento 467 dell'11 OTTOBRE 2018 [doc. web n. 9058979]:

1. Trattamenti valutativi o di scoring su larga

scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso App, relativi ad "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato";

2. Trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. *screening* dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi);
3. Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso App, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, TV interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza, etc.;
4. Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti);
5. Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici

(anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8);

6. Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo);
7. Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il Wi-Fi tracking) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01;
8. Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche;
9. Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment);
10. Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.
11. Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento;
12. Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

A livello generale un ingegnere professionista o uno studio associato che svolgono prevalentemente attività connesse al primo e al secondo settore dell'Ordine non dovrebbero avere trattamenti che rientrano nell'ambito di obbligatorietà di svolgimento di una DPIA a meno che:

- Abbiano o intendano avere una componente di attività non marginale connessa ad attività di Consulenze Tecniche di Parte (CTP) o Consulenze Tecniche d'Ufficio (CTU);
- Svolgano o intendano svolgere attività in ambito sanitario che li portino a trattare dati sensibili;

- Facciano uso o intendano fare uso "massiccio" di automazione per il trattamento di dati personali;
- Facciano uso o intendano fare uso di profilazione dei propri clienti (persone fisiche).

L'ingegnere professionista o lo studio associato che opera prevalentemente nel terzo settore può avere una situazione differente. Essendo meno "standard" le attività svolte in questo settore si rimanda a successivi approfondimenti e/o verticalizzazioni della presente guida. In ogni caso si presuppone che l'ingegnere professionista o studio associato che opera nel terzo settore abbia maggiore dimestichezza con gli aspetti di protezione delle informazioni.
Esula dallo scopo della presente linea guida, almeno in questa prima versione, fornire una metodologia di valutazione d'impatto per la protezione dei dati personali, ma si rimanda all'allegato 1 del WP248 per avere un'idea dei quadri europei esistenti sul tema, ciascuno dei quali può essere personalizzato per lo specifico titolare del trattamento oppure essere comune a un determinato settore di mercato.
Infine, qualora il Titolare del Trattamento non fosse in grado di trovare misure sufficienti per ridurre i rischi a un livello accettabile, ossia i rischi residui restano comunque elevati anche a fronte dell'implementazione delle contromisure risultati dalla valutazione effettuata, sarà necessario consultare l'autorità di controllo, come previsto dall'art. 36. L'autorità è tenuta a fornire, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto al Titolare del Trattamento e, ove applicabile, al Responsabile del Trattamento, periodo che potrà essere prorogato di sei settimane, tenendo conto della complessità del trattamento previsto. In caso di proroga il Titolare del Trattamento e, ove applicabile, il Responsabile del Trattamento saranno opportunamente informati, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione. La decorrenza dei termini può essere sospesa fino all'ottenimento da parte dell'autorità di controllo delle informazioni richieste ai fini della consultazione.

2.8 Data Protection by Design e by Default art. 25

I principi di Data Protection by Design e Data Protection by Default richiedono che la tutela dei diritti e delle libertà degli interessati con riguardo al trattamento dei dati personali comportino l'attuazione di adeguate misure tecniche e organizzative sia in fase di progettazione che dell'esecuzione del trattamento stesso, al fine di garantire il rispetto delle disposizioni del Regolamento.
In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone e che gli interessati siano messi in condizione di controllare la distribuzione dei propri dati personali.
Questi principi introducono una nuova concezione della protezione dei dati personali che non deve essere più essere intesa come qualcosa da applicare a posteriori sui trattamenti effettuati, bensì deve essere incorporata in tutte le fasi del ciclo di vita di qualsiasi tecnologia che tratti dati personali, assicurandone costantemente la tutela dei diritti e delle libertà delle persone. Tutela che trova il suo fondamento nel principio di "minimizzazione" sancito dall'art. 5 del regolamento, inteso nella sua accezione più ampia: ricorrere all'utilizzo del dato personale solo in casi estremi e strutturare i servizi che utilizzano nuove tecnologie in modo tale limitare al minimo i dati trattati rispetto alle finalità per le quali essi vengono acquisiti.
Nel contesto dell'ingegnere professionista o dello studio associato operante nell'ambito del primo e/o secondo settore, in prevalenza si adotteranno processi e sistemi standard a supporto e non sviluppati appositamente per la realtà specifica. Discorso differente potrebbe essere per ingegneri professionisti o studi associati che operano prevalentemente nel terzo settore dell'Ordine degli Ingegneri.
Il Regolamento si spinge nel proporre un meccanismo che permette il rispetto dei suddetti principi, la pseudonimizzazione, la minimizzazione e la cifratura dei dati personali[28].
Possibile implementazione pratica dei principi di Data Protection by Design e by Default nel contesto specifico dell'ingegnere professionista o dello studio associato operante nell'ambito del primo e/o secondo settore potrebbe essere la definizione di una Politica di Data Protection by Design che definisce cosa deve essere richiesto o verificato nell'acquisizione di sistemi dal mercato.
A tal proposito si propone di seguito un breve elenco di linee guida liberamente scaricabili dalla Rete:

- "Linee guida per lo sviluppo del software sicuro" pubblicato dall'Agenzia per l'Italia Digitale (AgID);
- "Privacy and Data Protection by Design – from policy to engineering", pubblicato da ENISA;
- "Software development with Data Protection by Design and by Default" pubblicato dal Garante norvegese;
- "Privacy by design" pubblicato dal Garante canadese (Ontario).

2.9 Gestione delle violazioni, notifiche all'autorità di controllo e all'interessato artt. 33-34

Per «violazione dei dati personali», anche nota come data breach, si intende 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 (art. 4 punto 12). La violazione dei dati personali, pertanto, non è solo un atto illecito (ad es. il furto di dati) ma rientrano nelle violazioni dei dati personali anche eventi interni all'organizzazione (ad es. lo smarrimento di una chiavetta USB, la rottura dell'hard disk su cui risiedono i dati dei clienti, ecc.).

La gestione delle violazioni dei dati personali può essere schematizzata in tre passi successivi (vedi figura 2):

1. Il primo è l'identificazione e gestione della violazione: lo scopo di questo primo passo è quello di identificare il prima possibile gli incidenti di sicurezza che possono generare una violazione dei dati personali e gestirne la risoluzione;
2. Il secondo è la valutazione dell'evento: lo scopo è quello di valutare la violazione e scalarla verso il Titolare del Trattamento qualora si agisca in qualità di Responsabile del Trattamento. Sarà in capo al Titolare la decisione se deve essere effettuata formalmente la notifica all'Autorità Garante e la eventuale comunicazione agli interessati;
3. Il terzo è la notifica formale all'Autorità Garante e la comunicazione agli interessati, se necessaria.

Le violazioni possono essere classificate in base ai seguenti principi della sicurezza delle informazioni:

- "violazione della riservatezza", ad es. in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;
- "violazione dell'integrità", ad es. in caso di modifica non autorizzata o accidentale dei dati personali;
- "violazione della disponibilità", ad es. in caso di perdita accidentale o non (anche temporanea) di dati personali.

A seconda dei casi, una violazione può riguardare contemporaneamente uno o più aspetti della riservatezza, l'integrità e la disponibilità dei dati personali.

Ciò premesso, l'art. 33 del Regolamento dispone che in caso di violazione dei dati personali, il Titolare del trattamento debba notificare la violazione all'autorità di controllo competente senza ingiustificato ritardo, ove possibile entro 72 ore dal momento in cui ne è venuto a conoscenza , a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora non sia effettuata entro 72 ore, la notifica all'autorità di controllo deve essere corredata di una giustificazione motivata del ritardo.

Tale notifica deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di in-

Figura 2

teressati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare il nome e i dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Il Titolare del Trattamento deve mantenere un registro in cui documentare qualsiasi violazione dei dati personali, incluse le circostanze in cui si è verificata, le sue conseguenze e i provvedimenti adottati per porvi rimedio. La documentazione deve consentire all'autorità di controllo di verificare il rispetto del regolamento.

Allorquando tale violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento comunica la violazione anche all'interessato senza ingiustificato ritardo (ai sensi dell'art. 34). La comunicazione della violazione dei dati personali alle persone interessate consente al Titolare del trattamento di fornire loro informazioni sui rischi derivanti dalla violazione e sui provvedimenti che esse possono prendere per proteggersi dalle potenziali conseguenze della violazione.

Per tale motivo la comunicazione deve descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contenere almeno le informazioni di cui sopra. Tuttavia, si è esentati dalla comunicazione verso l'interessato se:

a) il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazio-

ne, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, ad es. cifrando le informazioni o pseudonimizzandole (purché la tabella di transcodifica non sia stata anch'essa violata);

b) il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica (ad es. sui mass media) o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Qualora il libero professionista o lo studio professionale agisca in qualità di Responsabile, pur restando in capo al Titolare la responsabilità generale per la protezione dei dati personali e della notifica del data breach, è comunque tenuto a supportare il Titolare nel garantire il rispetto dei propri obblighi, segnatamente in materia di notifica delle violazioni, tenendo conto delle informazioni in suo possesso.

Se il libero professionista (o lo studio professionale) fornisce servizi a più titolari del trattamento tutti interessati dal medesimo incidente, dovrà segnalare i dettagli dell'incidente a ciascun Titolare (ad es. viene smarrito un notebook contenente i dati personali di più clienti senza che lo stesso sia stato adeguatamente protetto).

Data la complessità e delicatezza della questione dei data breach, il gruppo dei Garanti europei (EPDB) si è espresso con un'apposita linea guida WP250, nella quale viene diffusamente descritta la materia ed alla quale si rimanda per ulteriori approfondimenti, come anche alle Linee Guida 01/2021 in cui si riportano una serie di interessanti casistiche di data breach.

2.10 Trasferimento dei dati extra UE- trasferimento a terzi artt. 44-50

Il Regolamento dedica un'intera sezione (Capo V, artt. dal 44 al 50) al trasferimento dei dati personali all'estero. Come detto in apertura del presente documento il GDPR, così come la Direttiva 46/95/CE che ha sostituito, mira alla protezione dei dati personali ma anche a consentire la loro circolazione.

È opportuno sin da subito precisare che, per gli scopi della presente linea guida, tali disposizioni riguardano il libero professionista che per determinati motivi debba trasferire i dati personali dei propri clienti verso un paese terzo o organizzazione internazionale che si trovi al di fuori dell'Unione Europea, sia che esso operi come Titolare che come Responsabile del Trattamento. Questa evenienza è tutt'altro che remota in quanto è facile che un professionista utilizzi servizi gratuiti o a pagamento in cloud per l'archiviazione di dati (a titolo di esempio servizi quali Dropbox, GDrive, OneDrive, ecc.) o servizi di messaggistica (a titolo di esempio Skype, WhatsApp, Gmail, Telegram, Signal, ecc.).

La movimentazione dei dati fra paesi differenti è una disciplina articolata, per lo scopo di questa linea guida si deve tenere in considerazione quanto segue:

- La circolazione dei dati personali attraverso paesi dell'Unione Europea è liberamente consentita;
- Il trasferimento dei dati personali verso paesi extra UE è consentito se:
  - Il paese è un paese considerato trust dalla Commissione Europea;
  - La società fornitrice del servizio adotta le clausole contrattuali standard;
  - L'interessato ha fornito esplicito consenso al trasferimento dei dati in quei paesi specifici.

3. LE NOVITÀ INTRODOTTE DAL NUOVO REGOLAMENTO RISPETTO ALLA NORMATIVA PRECEDENTE

All'interno di questa sezione si vuole riportare un'indicazione delle principali novità, o cambiamenti, rispetto alla normativa precedentemente vigente in Italia, premettendo che non è mutata la filosofia alla base del GDPR e quella che era presente nella previgente Direttiva 46/95/CE. Si può affermare che il nuovo quadro normativo ha due obiettivi principali:

1. Favorire il processo di omogeneizzazione della normativa fra i diversi stati dell'Unione. Aspetti principali che sono stati seguiti sono: adozione della forma di Regolamento e non più di Direttiva, quindi eliminando la necessità di recepimento da parte degli stati membri dell'Unione; ufficializzazione del "Comitato europeo per la protezione dei dati" che ha, tra le sue responsabilità, quella di omogeneizzare le interpretazioni e i provvedimenti delle diverse autorità nazionali.
2. Aggiornare la normativa in modo da poter regolamentare servizi moderni fortemente digitalizzati, social network, mobile, ecc. che trasferiscono enormi quantità di dati personali verso paesi extra-UE, anche per attività di profilazione degli utenti.

Se il passaggio normativo europeo rimane coerente come filosofia, l'impatto in Italia - con riferimento alla precedente normativa - segna delle differenze significative. Un cambiamento importante è il passaggio dalla stringente indicazione delle "misure minime di sicurezza" (allegato B del DLgs 196/03 pre-GDPR) alla libertà di identificazione delle misure di sicurezza da parte del Titolare e del Responsabile. La precedente normativa italiana vincolava e guidava di più il Titolare nell'identificazione delle misure di sicurezza[30].
Il nuovo quadro normativo europeo ha introdotto un concetto più moderno di responsabilizzazione (*accountability*) del Titolare. Tale concetto fa riferimento a molteplici ed eterogenei aspetti, configurando la responsabilità come un insieme di prescrizioni da seguire secondo un approccio marcatamente *proattivo* alla protezione dei dati personali e non come mera applicazione di una lista di misure di sicurezza generiche e preconfezionate. Il Titolare è responsabilizzato nel prendere decisioni in merito alla protezione dei dati personali in modo analogo a quanto deciso in materia di business dell'organizzazione. La responsabilizzazione è una delle principali novità del nuovo quadro normativo. Per poter mettere in atto correttamente questo principio il Titolare del trattamento deve:

a. identificare e mettere in essere misure tecniche ed organizzative al fine di garantire un livello di sicurezza adeguato al rischio[31];
b. essere in grado di dimostrare la conformità dell'organizzazione e delle scelte prese e il rispetto del principio di *Data Protection by Design e by Default*.

Il Titolare ha la responsabilità di andare ad identificare e valutare i rischi possibili inerenti al trattamento dei dati personali, deve identificare le misure di sicurezza per la loro protezione affinché siano adeguate ai suddetti rischi e deve procedere al riesame ed eventuale aggiornamento quando necessario. Possibili strumenti atti a dimostrare il rispetto degli obblighi del Titolare sono l'adesione ai codici di condotta o a un meccanismo di certificazione .
Registro delle attività di trattamento, ex art. 30, in cui il Titolare deve riportare l'elenco dei trattamenti svolti, comprese le finalità dello stesso, i tipi di dati trattati, i soggetti interessati, le misure adottate etc. Il Registro delle Attività di Trattamento non è propriamente una novità introdotta dal GDPR in quanto questo adempimento era presente anche nella precedente normativa ed era stato formalizzato nel così detto Documento Programmatico della Sicurezza (DPS) . La formalizzazione del Registro delle Attività di Trattamento permette al Titolare e al Responsabile di dimostrare di avere sotto controllo il processo di trattamento dei dati personali e le misure di sicurezza messe in atto sugli specifici trattamenti. L'obbligatorietà della formalizzazione e mantenimento del Registro delle Attività di Trattamento non è generalizzata (vedi §3.3).

> *Nota:* l'art. 30 del GDPR punto 5 indica che sono esentate le imprese o organizzazioni con meno di 250 dipendenti, quindi l'ingegnere professionista o lo studio associato a cui è indirizzata la presente guida non sono obbligati a redigerlo e mantenerlo a meno che:
> - il trattamento che viene effettuato presenta un rischio per i diritti e le libertà degli interessati;
> - il trattamento non è occasionale;
> - il trattamento include categorie particolari di dati personali o dati personali relativi a condanne penali e a reati.
>
> L'ingegnere professionista o lo studio associato potrebbero rientrare nell'obbligatorietà della redazione del Registro delle Attività di Trattamento qualora svolgano attività per clienti che sono prevalentemente persone fisiche, ad es. quando coinvolti nello svolgimento di Consulenze Tecniche d'Ufficio (CTU) o Consulenze Tecniche di Parte (CTP).

Data Protection by Design e Data Protection by Default[34] (vedi § 3.7) sono due principi formalizzati a livello normativo nel GDPR che mirano alla creazione di un contesto strutturato all'interno del quale la protezione dei dati personali è

presa in considerazione sin dalle prime fasi di progettazione del trattamento e dei sistemi informativi che ne sono a supporto.

Nota: l'art. 25 del GDPR ha introdotto formalmente per la prima volta a livello normativo europeo questi due principi, benché non si tratti di concetti di nuova formulazione[35].

Il Data Protection by Default è relativo alla messa in atto di misure tecniche e organizzative necessarie a far sì che vengano trattati solo i dati pertinenti e limitati a quanto necessario rispetto alle finalità perseguite.

> *Consiglio:* l'applicazione dei due principi di Data Protection by Design e Data Protection by Default risulta essere complessa ed articolata con implicazioni significative soprattutto nel caso di sviluppo *ad-hoc* di processi e sistemi a supporto. Nel contesto specifico dell'ingegnere professionista e dello studio associato a cui è indirizzato questo documento è più probabile l'utilizzo di processi e sistemi standard di mercato quindi è possibile implementare questi due principi attraverso la formalizzazione di una politica che prevede la verifica del rispetto della loro applicazione nei processi e negli strumenti a supporto.

Importante novità introdotta dal nuovo quadro normativo è l'obbligatorietà della notifica all'Autorità Garante della Protezione dei Dati Personali in caso di violazione dei dati personali (art. 33 del GDPR) e, qualora non siano presenti specifici accorgimenti, anche agli interessati (vedi § 3.8). Per quanto riguarda il contesto nazionale questa non è una novità in senso assoluto, ma un'estensione a tutti i settori di quanto già presente in ambito sanitario, bancario, biometrico e delle telecomunicazioni.

Infine, il GDPR ha apportato significative novità anche in ordine al regime sanzionatorio, previsto in caso di inadempienza o violazione della normativa regolamentare.

L'entità della sanzione è stata sensibilmente incrementata rispetto alla precedente normativa sulla privacy (Dlgs 196/2003) e varia, ovviamente, a seconda del tipo di violazione. I massimali delle sanzioni sono ora:

- art. 83 paragrafo 4: la violazione delle disposizioni comporta una sanzione amministrativa pecuniaria fino a 10 milioni di euro o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore;
- art. 83 paragrafo 5: prevede sanzioni ancora più elevate, fino a 20 milioni di euro o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, in ragione della maggior gravità delle violazioni delle relative disposizioni;
- Art. 83 paragrafo 6: prevede le medesime sanzioni del paragrafo 5 nel caso di «inosservanza di un ordine da parte dell'autorità di controllo di cui all'articolo 58, paragrafo 2».

  Nota: l'art. 83 del GDPR riporta i massimali delle sanzioni che possono essere inflitte. Queste sono state radicalmente inasprite rispetto al regime precedente[36], sebbene ogni violazione avrà una sanzione non necessariamente pari al massimale, ma commisurata alla gravità della violazione stessa.

4. QUADRO NORMATIVO

L'obiettivo della presente sezione è quello di fornire una panoramica generale circa gli elementi importanti del GDPR attraverso una prospettiva che includa l'analisi del lato attivo e passivo del rapporto tra Titolare del trattamento e i cittadini (gli interessati) in merito al trattamento dei dati personali.

4.1 Sintesi dei principali riferimenti normativi e best practices connesse (vedere tabella 1)

Normativa	Data	Autore
REGOLAMENTO (UE) 2016/679 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 (regolamento generale sulla protezione dei dati)	27/04/2016	Parlamento Europeo e Consiglio
DIRETTIVA (UE) 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio	27/04/2016	Parlamento Europeo e Consiglio

Tabella 1

DECRETO LEGISLATIVO 30 giugno 2003, n.196 recante il "Codice in materia di protezione dei dati personali" emendato dal Dlgs. 101/2018	30/06/2003 (agg. 10/08/2018)	Parlamento
DECRETO LEGISLATIVO 10 agosto 2018, n. 101 Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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 (regolamento generale sulla protezione dei dati).	10/08/2018	Parlamento
DECRETO LEGISLATIVO 18 maggio 2018, n. 51 Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.	18/05/2018	Parlamento
Provvedimenti generali Garante Privacy (https://www.garanteprivacy.it/provvedimenti/provvedimenti-a-carattere-generale)	Varie	Garante per la protezione dei dati personali
UNI CEI EN ISO/IEC 27001:2017 Tecnologie Informatiche - Tecniche di sicurezza - Sistemi di gestione della sicurezza dell'informazione - Requisiti	23/01/2018	ISO/IEC - UNI
UNI CEI EN ISO/IEC 27002:2017 Tecnologie Informatiche - Tecniche di sicurezza - Codice di pratica per la gestione della sicurezza delle informazioni	30/03/2017	ISO/IEC - UNI
UNI/PdR 43.1:2018 Linee guida per la gestione dei dati personali in ambito ICT secondo il Regolamento UE 679/2016 (GDPR) - Gestione e monitoraggio dei dati personali in ambito ICT	11/09/2018	UNI
UNI/PdR 43.2:2018 Linee guida per la gestione dei dati personali in ambito ICT secondo il Regolamento UE 679/2016 (GDPR) - Requisiti per la protezione e valutazione di conformità dei dati personali in ambito ICT	11/09/2018	UNI
Misure minime di sicurezza ICT per le pubbliche amministrazioni		AgID
ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management —Requirements and guidelines	08/2019	ISO/IEC

5. DOMANDE FREQUENTI – FAQ

In questa sezione sono riportate delle FAQ relative alla protezione dei dati personali divise in sotto sezioni ovvero:

- SEZIONE 1: FAQ sulla normativa e sulle principali definizioni. In questa sezione sono riportate le definizioni principali riprese dalla normativa e alcune descrizioni/concetti che possono aiutare il lettore a navigare all'interno della normativa per approfondimenti.
- SEZIONE 2: Diritti degli interessati. In questa sezione sono riportati l'elenco completo dei diritti degli interessati (i cittadini) sia quelli che sono stati formalizzati dalla normativa come "nuovi diritti", sia quelli che erano già stati formalizzati nel corso del tempo dalla giurisprudenza nazionale o Europea.
- SEZIONE 3: Doveri del titolare del trattamento e del responsabile del trattamento. In questa sezione sono riportati le responsabilità del Titolare del Trattamento e del Responsabile del Trattamento con una descrizione di ciò che queste attività possono significare. Ove possibile è stato inserito un esempio contestualizzato al caso degli Ingegneri.
- SEZIONE 4: Esempi pratici nel contesto degli Ingegneri. In questa sezione è stata

riportata la risposta ad alcune domande che possono sorgere ad un ingegnere nella sua normale attività professionale.

- SEZIONE 5: FAQ di alcune delle Autorità Europee Garanti della Protezione dei Dati Personali. In questa sezione sono state riportate fedelmente le FAQ del Garante Italiano della Protezione dei Dati Personali, la traduzione di quelle del Garante francese e di quello inglese.

Al fine di agevolare approfondimenti del lettore sono stati inseriti i riferimenti alla normativa sulla protezione dei dati personali nazionale o europea.

5.1 Sezione 1: FAQ sulla normativa e sulle principali definizioni

ID Q	Domanda	ID R	Risposta
Q.1.	Qual è la base normativa attuale di riferimento sulla Protezione dei Dati Personali?	**R.1.**	La base normativa è articolata su un mix di norme alcune a livello europeo ed altre a livello nazionale. La base normativa per eccellenza è la Carta dei Diritti Fondamentali dell'Unione Europea (articolo 8), a questo si aggiunge il Regolamento UE 679/2016 (da qui in avanti GDPR), la Direttiva UE 680/2016 e il suo recepimento in Italia attraverso la D.lgs. 51/2018, il D.lgs. 196/2003 modificato dal D.lgs. 101/2018, le *Opinion* e i pareri del Comitato Europeo per la Protezione dei Dati, i Provvedimenti generali ed i pareri dell'Autorità Garante della Protezione dei Dati Personali italiana. A queste si aggiunge la Direttiva UE 58/2002 (recepita dal D.lgs. 196/2003).
Q.2.	Che cos'è un dato personale?	**R.2.**	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. (Articolo 4, Considerando 26, 27 e 30 – GDPR) Esempi di dato personale sono: • Nome e Cognome; • Codice Fiscale; • Fotografia; • Registrazioni video; • Numero di matricola di una persona; • Indirizzo mail; • Numero telefono fisso o mobile; • Account social network/messaging; • Ecc.
Q.3.	Che cosa sono le "categorie particolari di dati personali" (dati sensibili)?	**R.3.**	Sono quei dati personali, generalmente indicati come **sensibili**, atti a rilevare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché 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. (Articolo 9, Considerando 51, 52 e 53 – GDPR) Esempi di categoria particolare di dato personale sono: • Cartella clinica/risultato analisi cliniche; • Iscrizione a sindacati; • Certificati di invalidità civile; • Cartella clinica/risultato analisi cliniche; • Ecc.

ID Q	Domanda	ID R	Risposta
Q.4.	Che cosa sono i "dati giudiziari"?	**R.4.**	I dati giudiziari corrispondono ai dati personali relativi a condanne penali e ai reati. Tali dati possono essere trattati solo 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 può essere tenuto solo sotto il controllo dell'autorità pubblica.
Q.5.	I dati relativi ai minori rientrano nelle categorie particolari?	**R.5.**	No. I dati dei minori non costituiscono una categoria particolare di dato personale e vengono trattati come tutti gli altri dati personali, fatta eccezione per il consenso che deve essere autorizzato dai genitori, o del tutore, nel caso di minori con età inferiore ai 16 anni. (Articolo 8, para 1, lett. a, Considerando 38 – GDPR) o 14 anni (art'8 par. 2 - GDPR) nei casi previsti dall'Art.2 2-quinquies para 1 del D.lgs. 196.
Q.6.	Che cos'è un trattamento?	**R.6.**	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. (Articolo 4 – GDPR)
Q.7.	Quali sono le informazioni da fornire all'interessato e quando?	**R.7.**	Quando i dati personali di un soggetto, detto "interessato" sono oggetto di un trattamento, richiesto o meno dal soggetto stesso, a questi deve essere fornita un'informativa che contenga almeno le seguenti informazioni, come stabilito dagli articoli 13 e 14 del GDPR: • Chi è l'interessato • Chi effettua il trattamento • Se nominato, i recapiti del DPO • Quali sono i trattamenti effettuati e perché • Qual è la base giuridica del trattamento • Quali sono i dati raccolti • Se il trattamento comporta operazioni automatizzate, come la profilazione • Se i dati verranno comunicati a soggetti esterne (responsabili esterni) • Per quanto tempo saranno conservati e in che modo • Se i dati saranno trasferiti in altri Paesi e come • Quali sono i diritti dell'interessato.
Q.8.	Che cos'è la profilazione?	**R.8.**	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. (Articolo 4, Considerando 24, 30, 71 e 72 – GDPR)
Q.9.	Che cos'è la Pseudonimizzazione?	**R.9.**	Fare in modo 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. (Articolo 4, Considerando 26, 28 e

ID Q	Domanda	ID R	Risposta
Q.10.	Quando un dato può essere considerato anonimo?	**R.10.**	Un dato è anonimo quando non si riferisce a una persona fisica identificata o identificabile o è reso sufficientemente anonimo da impedire o da non consentire più l'identificazione dell'interessato. (Considerando 26 – GDPR)
Q.11.	Che cos'è la limitazione del trattamento e quando va applicata?	**R.11.**	Per limitazione si intende la possibilità di contrassegnare i dati personali conservati con l'obiettivo di limitarne temporaneamente il trattamento. Questa limitazione dovrà essere tenuta in considerazione soprattutto da chi si occupa della progettazione dei sistemi informativi: "by design" infatti sarà necessario prevedere una funzionalità di questo tipo, che permetta di "contrassegnare" i dati personali memorizzati, il cui trattamento potrà essere limitato potenzialmente in qualunque momento da parte dell'interessato o dell'Autorità Garante. Si tratta di una sorta di sospensione temporanea del trattamento in corso che però può presentare delle eccezioni (per approfondimenti: Art. 18 e Considerando 67 - GDPR, Art. 2-undieces – D.lgs. 196)
Q.12.	Che cosa si intende per "Archivio"?	**R.12.**	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. (Art. 4 e Considerando 15 - GDPR)
Q.13.	Che cos'è il Consenso?	**R.13.**	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. (Art. 4, Considerando 32 e 33 - GDPR)
Q.14.	Chi può dare il consenso?	**R.14.**	L'interessato (persona fisica) di cui si stanno trattando i dati personali (Art. 7, Considerando 42 e 43 - Regolamento UE 679/2016 – GDPR). Il minore con età minima di 14 anni può fornire il consenso **unicamente per l'offerta diretta di servizi della società dell'informazione** ai minori (Dlgs 196, Art. 2-quinquies para 1).
Q.15.	In quali forme può essere espresso il consenso?	**R.15.**	Nel caso di dati personali, non sensibili, può essere raccolto attraverso una dichiarazione scritta o (registrata), anche per via elettronica, che tuttavia deve comunicare chiaramente un atto affermativo. Per tutti i dati sensibili sarà necessario un consenso esplicito dell'interessato. Il consenso deve sempre essere libero, specifico, informato e non tacito o presunto, oltre che inequivocabile. Viene esclusa ogni forma di consenso tacito (il silenzio, cioè, non equivale al consenso) oppure ottenuto proponendo a un interessato una serie di opzioni già selezionate.
Q.16.	Chi è l'Interessato?	**R.16.**	L'interessato al trattamento dei dati è, in estrema sintesi, la persona fisica cui si riferiscono i dati personali oggetto di trattamento. Più precisamente, l'interessato è una persona fisica identificata o identificabile, direttamente o indirettamente facendo riferimento, ad esempio, ad informazioni come: il nome, un numero di identificazione, dati riguardanti l'ubicazione, un identificativo on-line oppure uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

ID Q	Domanda	ID R	Risposta
Q.17.	Chi è il Titolare del Trattamento?	**R.17.**	il Titolare del Trattamento (semplicemente Titolare) è la persona fisica, l'autorità pubblica, l'impresa, l'ente pubblico o privato, l'associazione, professionista, studio associato, ecc., che definisce le finalità e i mezzi del trattamento (art. 4, paragrafo 1, punto 7, del GDPR). L'Ingegnere libero professionista o lo studio associato rispetto al trattamento dei dati personali può ricoprire il ruolo di Titolare del Trattamento per quanto riguarda il trattamento dei dati dei propri clienti (persone fisiche).
Q.18.	Chi è il Responsabile del Trattamento?	**R.18.**	il Responsabile del Trattamento (semplicemente Responsabile) è la persona fisica o giuridica esterna al Titolare al quale questo affida specifici e definiti compiti di gestione e controllo svolti per suo conto e sotto sue indicazioni (art. 4, paragrafo 1, punto 8, del GDPR). L'Ingegnere libero professionista o lo studio associato rispetto al trattamento dei dati personali può ricoprire il ruolo di Responsabile del Trattamento per quanto riguarda il trattamento dei dati per conto di un suo cliente (azienda o organizzazione) nel quale opera sulla base di specifici contratti.
Q.19.	Chi è il Contitolare del Trattamento?	**R.19.**	Art. 26, par 1 del GDPR: *Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento.* Ciò deve essere formalizzato in un accordo interno in cui vengono specificate le rispettive responsabilità. L'Ingegnere libero professionista o lo studio associato rispetto al trattamento dei dati personali può ricoprire il ruolo di Contitolare, allorché determina congiuntamente ad altro Titolare finalità e mezzi del trattamento.
Q.20.	Chi è il Responsabile della Protezione dei Dati Personali/Data Protection Officer?	**R.20.**	Il responsabile della protezione dei dati (altrimenti detto Data Protection Officer, o DPO) è un consulente o un dipendente (esente da conflitti di interesse), esperto e qualificato, che affianca il titolare nella gestione delle questioni connesse al trattamento dei dati personali e lo aiuta a rispettare la normativa vigente. (Artt. 37-39, Considerando 97 - Regolamento UE 679/2016 – GDPR)
Q.21.	Quando va nominato il DPO?	**R.21.**	Come stabilito dall'art. 37 del GDPR, il DPO deve essere nominato obbligatoriamente dal titolare del trattamento o dal responsabile del trattamento in una serie definita di ipotesi. In primo luogo, nel caso in cui il trattamento dei dati sia effettuato da un'autorità pubblica o da un organismo pubblico, fatta eccezione per le autorità giurisdizionali quando esercitano le loro funzioni. Poiché nel Regolamento non viene data alcuna definizione specifica di "autorità pubblica" o di "organismo pubblico", il Gruppo di lavoro ex art. 29 ha ritenuto che questa definizione dovrà essere interpretata in conformità al diritto di ciascuno Stato membro. Si raccomanda, inoltre, la nomina di un DPO anche all'interno di quegli organismi privati incaricati dello svolgimento di funzioni pubbliche, o che comunque esercitano pubblici poteri (ad esempio, nel settore dei trasporti pubblici, delle forniture elettriche, delle infrastrutture stradali e così via). Infine, è opportuno che il DPO, una volta nominato, svolga la propria attività non solo con riferimento ai trattamenti strettamente connessi alle funzioni pubbliche dell'organismo, ma anche con riguardo ad altre attività, come la gestione di un database del personale. In secondo luogo, la nomina del DPO è obbligatoria quando le attività principali svolte del titolare o del responsabile del trattamento

ID Q	Domanda	ID R	Risposta
			consistono in operazioni che, per la loro natura, l'ambito di applicazione o le finalità, richiedono un monitoraggio regolare e sistematico degli interessati su larga scala. Il Gruppo di lavoro ex art. 29 raccomanda, per valutare il ricorrere o meno di questa circostanza nella situazione concreta, di tenere conto di una serie di fattori, fra i quali, a titolo esemplificativo, rilevano il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento, il volume dei dati e le diverse tipologie di dati che sono oggetto di trattamento, la durata o la persistenza dell'attività di trattamento e, infine, la portata geografica dell'attività di trattamento.
Q.22.	Che cosa deve essere garantito per proteggere adeguatamente i Dati Personali?	**R.22.**	La Riservatezza, l'Integrità, la Disponibilità e la Resilienza dei dati personali basata sull'analisi del rischio (art. 32 GDPR).
Q.23.	Che cos'è la Riservatezza del Dato Personale?	**R.23.**	La Riservatezza, o *Confidentiality*, del dato personale è la proprietà per cui il dato non è reso disponibile o rivelato a individui, entità o processi non autorizzati.
Q.24.	Che cos'è l'Integrità del Dato Personale?	**R.24.**	L'integrità, o *Integrity*, del dato personale è la proprietà relativa alla salvaguardia dell'accuratezza e della completezza di tali dati.
Q.25.	Che cos'è la Disponibilità del Dato Personale?	**R.25.**	La Disponibilità, o *Availability*, del dato personale è la proprietà di essere accessibile e utilizzabile quando necessario, anche su richiesta di un'entità autorizzata.
Q.26.	Che cos'è la Resilienza del Dato Personale?	**R.26.**	Il GDPR fa riferimento, nell'art. 32, al concetto di resilienza dei sistemi e dei servizi informatici che trattano i dati personali. Questo concetto si riferisce, in termini molto generali, alla capacità intrinseca di un sistema di adattarsi alle condizioni d'uso e di resistere all'usura al fine di assicurare sempre la disponibilità dei servizi che vengono forniti e la adeguata protezione dei dati che vengono trattati con tali sistemi.
Q.27.	Che cos'è la Data Protection Impact Assessment?	**R.27.**	La Data Protection Impact Assessment, o Valutazione di Impatto, è un processo che permette al titolare del trattamento di valutare la necessità, la proporzionalità ed i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali, così da approntare misure idonee di sicurezza. Tale processo è inoltre espressione del principio di responsabilizzazione (accountability) del titolare nei confronti dei trattamenti da questo effettuati. (Art. 35 GDPR).
Q.28.	Quando va svolta la Data Protection Impact Assessment?	**R.28.**	La valutazione è necessaria quando il trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche e va fatta, in particolare, in alcuni specifici casi previsti dal GDPR e cioè in presenza di un monitoraggio sistematico dei dati o di una sorveglianza sistematica su una zona accessibile al pubblico o quando i dati sensibili sono trattati su larga scala. Il Gruppo Art. 29 (wp248) individua 9 criteri specifici: • trattamenti valutativi o di scoring, compresa la profilazione; • decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni); • monitoraggio sistematico (es: videosorveglianza); • trattamento di dati sensibili, giudiziari o di natura estremamente personale (es: informazioni sulle opinioni politiche);

ID Q	Domanda	ID R	Risposta
			• trattamenti di dati personali su larga scala; • combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data); • dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.); • utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, device IoT, ecc.); • trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento). Il Garante, con il provvedimento n.467 dell'11 Ottobre 2018 ha aggiunto ai precedenti altri criteri per cui è obbligatoria la DPIA, ovvero: • Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse. • Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento. • Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento. **NOTA**: La DPIA è necessaria in presenza di almeno due di tutti i criteri sopra elencati, ma - tenendo conto delle circostanze - il titolare può decidere di condurre una DPIA anche se ricorre uno solo dei criteri di cui sopra. Nel contesto specifico degli ingegneri professionisti o degli studi associati un tipico trattamento per il quale deve essere svolta una DPIA è la videosorveglianza.

5.2 Sezione 2: Diritti degli Interessati

ID Q	Domanda	ID R	Risposta
Q.29.	Il GDPR ha formalizzato una serie di diritti per qli interessati, quali sono le modalità di esercizio di questi diritti per gli Interessati?	**R.29.**	Le modalità per l'esercizio di tutti i diritti da parte degli interessati sono stabilite, in via generale, negli artt. 11 (Trattamento che non richiede l'identificazione) e 12 (Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato) del regolamento. Nel contesto specifico degli ingegneri professionisti o degli studi associati visto la dimensione limitata degli stessi un possibile metodo è quello di comunicare delle informazioni di contatto dove poter esercitare i propri diritti (ad esempio: indirizzo dello studio, indirizzo email dedicato a tematiche privacy e recapito telefonico).
Q.30.	In che modo il titolare comunica all'interessato come intende trattare i suoi dati? Il titolare deve specificare come tratta i dati dell'interessato?	**R.30.**	Attraverso un'informativa in cui viene specificato: come vengono trattati i dati, per quali finalità, come vengono tutelati, le modalità di cancellazione e di reclamo. (Artt. 13 e 14 del GDPR) Il titolare è tenuto ad adottare misure appropriate per fornire all'interessato tutte le informazioni/comunicazioni relative ai trattamenti gestiti dalla propria organizzazione, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. Il titolare è tenuto ad agevolare l'esercizio dei diritti da parte dell'interessato e, in particolare, a fornire un riscontro alla richiesta del medesimo senza ingiustificato ritardo e comunque entro un mese dal ricevimento della medesima (prorogabile di due mesi ove necessario, tenuto conto della complessità e del numero delle richieste). (principio di Trasparenza, Art. 12 GDPR)
Q.31.	Quali sono i diritti per gli interessati?	**R.31.**	I diritti dell'Interessato sono disciplinati dal Capo III del GDPR e in particolare dagli artt. 12-23. I diritti per l'Interessato sono: Diritto di accesso (Art. 15), diritto di rettifica (Art. 16), diritto alla cancellazione (Art. 17), diritto di limitazione del trattamento (Art. 18), diritto alla portabilità (Art. 20), Diritto di opposizione (Art. 21). L'esercizio di tali diritti è disciplinato dall'Art. 12 con le limitazioni previste dall'Art. 23, meglio specificati dagli art. 2-undecies e 2-duodecies del nuovo Codice Privacy. Nel caso in cui il Trattamento non richieda l'identificazione dell'Interessato, decadono gli articoli 15-23 e quindi l'esercizio degli stessi da parte dell'Interessato.
Q.32.	Cos'è il Diritto di Accesso? Cosa cambia rispetto al D.Lgs. 196/2003?	**R.32.**	Il diritto di accesso è disciplinato dall'Art. 15 del GDPR, secondo il quale l'Interessato ha il diritto di accedere ai dati ed alle informazioni, quali: • finalità del trattamento • categorie di dati personali oggetto di trattamento • destinatari a cui sono o saranno comunicati i dati personali (nel caso di Paesi Terzi o organizzazioni internazionali fare riferimento all'art. 46) • periodo di conservazione dei dati personali previsto • possibilità di chiedere l'esercizio dei diritti di cancellazione o rettifica o limitazione • diritto di reclamo al Garante • le informazioni sull'origine della raccolta dei dati personali, se i dati non sono stati raccolti presso l'interessato • informazioni sul processo decisionale automatizzato, se presente, e su come viene utilizzato
Q.33.	Cos'è il Diritto di Rettifica	**R.33.**	l'art. 16 GDPR contiene una specifica e autonoma disposizione che assegna all'interessato il diritto di rettifica, inteso come rettifica dei dati personali che lo riguardano e detenuti dal titolare. strumento di tutela del più ampio diritto all'identità personale, vale a dire del

ID Q.	Domanda	ID R	Risposta
			diritto alla veritiera rappresentazione della propria personalità agli altri, senza alterazioni o travisamenti. Oggetto di questo diritto sono tutte le componenti dell'identità personale: da quelle fisico-corporali e psichico-caratteriali a quelle affettivo-comportamentali, dalle situazioni materiali alle relazioni interpersonali. La richiesta di rettifica può essere presentata dall'interessato senza particolari formalità, secondo modalità tradizionali (posta cartacea) o elettroniche (a mezzo mail o attraverso l'invio di un form web). Il titolare è tenuto ad adempiere senza ritardo e, comunque, entro un mese dal ricevimento dell'istanza di rettifica, a meno che - per la complessità dell'operazione richiesta - non sia necessario un termine più lungo per soddisfare i diritti dell'interessato. In tal caso, il titolare potrà disporre la rettifica richiesta entro il termine complessivo di tre mesi, ma tale proroga è ammessa previa comunicazione all'interessato. Se è possibile e non implica uno sforzo sproporzionato, il titolare comunica le rettifiche ricevute a ciascuno dei destinatari a cui sono stati eventualmente trasmessi i dati personali in questione. Nel caso in cui il titolare - eventualmente anche all'esito di richieste di chiarimenti all'interessato - decida di non dare corso alla richiesta, deve comunque rispondere nel termine di trenta giorni indicando le motivazioni e informando il richiedente della possibilità di proporre reclamo all'Autorità di controllo o di formulare ricorso all'Autorità giudiziaria ordinaria.
Q.34.	Cos'è il diritto di Cancellazione (o diritto all'oblio)? Cosa cambia rispetto al D.Lgs. 196/2003?	**R.34.**	In base all'art. 17, par. 1, il diritto di chiedere ed ottenere la cancellazione dei dati può essere esercitato dall'interessato solo al ricorrere dei seguenti motivi: • i dati personali eccedono le finalità per i quali sono stati raccolti o trattati; • subentra la revoca del consenso, già precedentemente rilasciato, salvo le deroghe e le esenzioni quali quelle previste in caso di trattamento a scopi giornalistici; • l'interessato esercita il diritto di opposizione (art. 21, parr. 1 e 2, GDPR); • l'eliminazione dei dati personali derivi da un obbligo legale dettato dal diritto dell'UE o dello Stato Membro in cui ha sede il titolare del trattamento; • i dati sono stati trattati illecitamente; • I dati sono stati raccolti per finalità legate all'offerta di servizi della società dell'informazione diretti a minori (art. 8, par. 1, GDPR).
Q.35.	Cos'è il diritto di limitazione del trattamento? Cosa cambia rispetto al D.Lgs. 196/2003?	**R.35.**	Il diritto di limitazione è disciplinato dall'art. 18 del GDPR e prevede che sia esercitabile: in caso di violazione dei presupposti di liceità del trattamento (come era già previsto dall'Art. 7 della 196/20013); se l'interessato è in attesa della rettifica dei dati richiesta al titolare dei dati 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).
Q.36.	Cos'è il Diritto alla Portabilità? Cosa cambia rispetto al D.Lgs 196/2003?	**R.36.**	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).

ID Q	Domanda	ID R	Risposta
			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 (si veda il considerando 68 ed il WP242 per maggiori dettagli). Inoltre, il titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, se tecnicamente possibile.
Q.37.	Cos'è il Diritto di Opposizione?	**R.37.**	Il diritto di opposizione, Art. 21 del GDPR, sancisce 4 possibili casi in cui l'Interessato può "opporsi" al trattamento dei dati personali (premesso che non è stato richiesto un preventivo consenso all'Interessato): • prima ipotesi: i dati personali sono trattati (anche per la profilazione) per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (art. 6, par. 1, lett. e) del GDPR). • seconda ipotesi: il trattamento dei dati considerato lecito ai sensi dell'art. 6 del Regolamento in quanto lo stesso è necessario per il perseguimento di un legittimo interesse del titolare del trattamento o di terzi (art. 6, par. 1, lett. f) del GDPR). • terza ipotesi: i dati sono trattati per finalità di marketing diretto. • quarta ed ultima ipotesi: i dati personali sono trattati a fini di ricerca scientifica, storica o statistica a norma dell'art. 89, par. 1, del Regolamento. La terza ipotesi è l'unica in cui l'interessato non è tenuto a fornire particolari motivazioni circa la propria opposizione e il titolare non può rifiutare la richiesta di opposizione.

5.3 Sezione 3: Doveri del Titolare del Trattamento e del Responsabile del Trattamento

ID Q	Domanda	ID R	Risposta
Q.38.	Come devono essere trattati i dati personali?	**R.38.**	I dati debbono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato. Le finalità devono essere determinate, esplicite e legittime; i dati: adeguati, pertinenti, esatti ed aggiornati, limitati a quanto necessario rispetto alle finalità, adeguatamente conservati e messi in sicurezza. (Art. 5 GDPR).
Q.39.	In che modo deve essere chiesto all'interessato il consenso al trattamento dei dati personali?	**R.39.**	(C32 del GDPR): "Il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il

ID Q	Domanda	ID R	Risposta
			trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso."
Q.40.	La richiesta del consenso è sempre obbligatoria?	**R.40.**	Il consenso non è sempre obbligatorio, come specificato nell'Art. 7 par. 4 del GDPR e nel C43 dello stesso. In particolare, laddove il trattamento sia indispensabile per l'esecuzione del contratto, esso non dovrà basarsi sul consenso ma sul diverso requisito della funzionalità ai fini negoziali.
Q.41.	Come deve essere chiesto il consenso in caso di minori?	**R.41.**	Nei casi in cui è richiesto il consenso, il trattamento di dati relativo all'offerta diretta di servizi della società dell'informazione ai minori è lecito se il minore che ha prestato il consenso ha compiuto 14 anni. In caso di minori di 14 anni, deve essere acquisito il consenso chi esercita la responsabilità genitoriale. (Art. 8 GDPR - Art. 2-quinquies DLgs 196/2003).
Q.42.	Nel caso di dati sensibili il titolare può chiedere il consenso al trattamento?	**R.42.**	Il titolare può chiedere il consenso esplicito per il trattamento di dati sensibili almeno nei seguenti casi: • l'interessato ha prestato il consenso esplicito; • i dati sono trattati per eseguire un contratto di lavoro e per le connesse esigenze di sicurezza/protezione sociale; • i dati sono trattati a fini di tutela di un interesse vitale dell'interessato; • i dati personali sono stati resi pubblici dall'interessato (Art. 9 del GDPR)
Q.43.	Cosa deve fare per mettere al sicuro i dati dell'interessato?	**R.43.**	Il Titolare deve adottare misure tecniche e organizzative adeguate al fine di garantire, ed essere in grado di dimostrare, la conformità del trattamento al Regolamento, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche. Le dette misure debbono essere periodicamente riesaminate e aggiornate. (Artt. 24, 32 GDPR)
Q.44.	In che modo il titolare può proteggere i dati dell'interessato?	**R.44.**	Attraverso i principi di Privacy by design e privacy by default, ovvero: 1. Tenendo conto delle specifiche caratteristiche del trattamento e dei connessi profili di rischio per i diritti e le libertà delle persone fisiche, all'atto del trattamento ovvero di determinare i mezzi del medesimo il titolare adotta misure tecniche e organizzative adeguate, in modo da attuare efficacemente i principi di protezione dei dati e da garantire nel trattamento i requisiti del Regolamento e la tutela dei diritti degli interessati. (Privacy by Design) 2. Il titolare del trattamento attua misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ciascuna finalità del trattamento. Obbligo che vale per la quantità dei dati raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità ai dati stessi. (Privacy by Default) (Art. 25 GDPR)
Q.45.	In quali casi il titolare deve effettuare delle nomine tramite un contratto?	**R.45.**	Il Titolare deve obbligatoriamente redigere un contratto nel caso in cui si trovi a nominare le figure Contitolare del trattamento, Responsabile del trattamento e Rappresentante del titolare. (Artt. 26,27 e 28 GDPR).

ID Q	Domanda	ID R	Risposta
			Nel contesto dell'ingegnere professionista o dello studio associato questa situazione potrebbe presentarsi nel caso in cui si ha una società che supporta la parte IT dell'ufficio, gestisce le buste paga dei dipendenti. Nel caso della gestione contabile attraverso uno studio Commercialista si ha che questi possono essere connotati come Titolari autonomi in funzione delle responsabilità che hanno.
Q.46.	In quali casi il titolare deve adottare obbligatoriamente un registro delle attività di trattamento?	**R.46.**	>250 dipendenti o larga scala o trattamento di dati sensibili. È adempimento obbligatorio per il titolare del trattamento con almeno 250 dipendenti o che, anche al di sotto di tale soglia dimensionale, effettui un trattamento che possa presentare un rischio per i diritti e le libertà degli interessati che non sia occasionale o che includa dati sensibili, genetici, biometrici, giudiziari. Cuore del documento è una mappa dettagliata di tutti i trattamenti effettuati dall'organizzazione del titolare. (art. 30 GDPR)
Q.47.	In quali casi il titolare deve inviare comunicazioni ufficiali all'Autorità di Controllo e in che modo?	**R.47.**	Nel caso di violazione dei dati personali. **Notificazione di una violazione dei dati** Rientra tra gli obblighi del titolare anche la notifica all'autorità di controllo (Garante) senza ingiustificato ritardo - e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza -, di ogni violazione della sicurezza dei dati personali che presenti un rischio per i diritti e le libertà delle persone fisiche. (Art. 33 GDPR)
Q.48.	Nel caso di violazione dei dati personali, il titolare deve sempre comunicarla all'interessato?	**R.48.**	**Comunicazione di una violazione dei dati all'interessato** Quando la violazione della sicurezza dei dati presenta un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare deve darne notizia all'interessato senza ingiustificato ritardo. La norma fissa i requisiti di contenuto della comunicazione, che deve essere redatta con un linguaggio semplice e chiaro. Altresì la norma individua i casi in cui la detta comunicazione non è richiesta (per semplicità, quando il titolare ha adottato misure tali da scongiurare il rischio o quando la comunicazione richiederebbe sforzi sproporzionati. In tal caso si procede ad una comunicazione pubblica o ad una misura simile con analoga efficacia. (Art. 34 GDPR)
Q.49.	In caso di violazione dei dati, il titolare deve sempre risarcire i danni?	**R.49.**	Il titolare è tenuto a risarcire il danno materiale o immateriale cagionato da una violazione del Regolamento. Egli è esonerato da tale responsabilità soltanto se dimostra che l'evento dannoso non gli è in alcun modo imputabile. (Art. 82 GDPR)
Q.50.	In quali casi il titolare deve organizzarsi per la valutazione di impatto (DPIA)?	**R.50.**	La valutazione di impatto (DPIA) è obbligatoria per il titolare nel caso in cui debba iniziare un trattamento molto rischioso per i diritti e le libertà delle persone fisiche. Ciò si può verificare, in particolare, quando sia implicato l'uso di nuove tecnologie, ovvero in considerazione di altre caratteristiche (natura, oggetto, contesto, finalità) del trattamento. Quando la valutazione di impatto indichi che il trattamento presenta un rischio elevato, prima di procedere al trattamento il titolare è tenuto a consultare l'autorità di controllo. (Artt. 35 e 36 GDPR)
Q.51.	In quali casi il titolare deve nominare un DPO?	**R.51.**	La nomina del DPO è adempimento obbligatorio quando il titolare del trattamento: a) è autorità/organismo pubblico (eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali); b) effettua trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; c) effettua come attività principali trattamenti su larga scala di dati sensibili, genetici, biometrici, giudiziari. Il DPO ha compiti di informazione, formazione,

ID Q	Domanda	ID R	Risposta
			consulenza e sorveglianza dell'adempimento della disciplina 'privacy'. E' anche l'interlocutore dell'autorità di controllo. (Art. 37, 38 e 39 GDPR) Nel contesto dell'ingegnere professionista o dello studio associato è molto probabile che non rientra nell'obbligo di nomina del DPO a meno di casi particolari come ad esempio se tratta dati sensibili.

5.4 Sezione 4: Esempi pratici

ID Q	Domanda	ID R	Risposta
Q.52.	Sono un ingegnere e svolgo attività di Direzione dei Lavori presso dei cantieri. Per motivi organizzativi mi vengono comunicati eventuali invalidità temporanee del personale in modo tale da impiegarlo in mansioni che non gli creano problemi. Inoltre, per la sicurezza del personale che opera nel cantiere il personale che utilizza alcune tipologie di macchinari viene sottoposto a test a sorpresa relativamente all'utilizzo di alcol e droghe in quanto potrebbe essere pericoloso. Devo adottare degli accorgimenti particolari?	**R.52.**	Informazioni relative alla salute (come le invalidità anche temporanee) così come i risultati dei test di uso di alcol o droghe rientrano nella sfera delle particolari categorie di dati personali (dati sensibili). Vedendo l'Art. 30 del GDPR si ha che in questo caso si rientra nell'obbligatorietà del mantenimento del Registro delle attività di trattamento. *Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con **meno di 250 dipendenti**, **a meno che** il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, **il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati** di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.* Essendo dati sensibili il professionista deve redigere un Registro dei trattamenti e, essendo dati sensibili, probabilmente rientrerebbe nell'obbligatorietà di redigere una DPIA e di implementare delle misure di sicurezza di un livello più elevato. Il GDPR suggerisce l'applicazione di un principio che è quello di minimizzazione quindi quello che si suggerirebbe di fare è: 1. È necessario che, come Direttore dei Lavori, si sia a conoscenza di tali dati? È possibile che di queste informazioni sia a conoscenza solo la società datrice di lavoro delle persone? 2. È possibile desensibilizzare queste informazioni (ad esempio non sapendo il risultato del test ma solo che è idoneo o non idoneo)? Le azioni da fare per trattare correttamente i dati sono: a. Redigere un Registro delle Attività di trattamento che includa il trattamento indicato; b. Formalizzare la nomina a Responsabile del Trattamento da parte della società titolare del cantiere; c. Applicare le misure di sicurezza richieste da parte della società titolare del cantiere; d. Avere un'accortezza nel trattare queste informazioni tenendo in considerazione la non diffusione a personale non autorizzato (ad esempio altro personale presente nel cantiere).

ID Q	Domanda	ID R	Risposta
Q.53.	Svolgo attività di CTU e CTP in diversi tribunali. Per lo svolgimento dei miei compiti ho la necessità di visionare della documentazione che mi è stata assegnata dal tribunale. Questa documentazione spesso è in formato cartaceo e non digitale. Non devo fare nulla essendo solo documentazione cartacea?	**R.53.**	Il GDPR vuole proteggere il trattamento dei dati personali indipendentemente dal formato con cui sono trattati, quindi è indifferente che siano in formato elettronico o cartaceo. Ovviamente le misure di sicurezza sono differenti in funzione del formato. Va tenuto presente che bisogna andare a proteggere tre aspetti principali dei dati personali che sono la Riservatezza, l'Integrità, la Disponibilità e la Resilienza. Nel caso di un'attività di CTP e CTU riveste particolare importanza la Riservatezza dell'informazione in quanto è probabile che le informazioni che siano trattate siano delle copie e non degli originali. È importante distinguere fra i due casi CTU o CTP, la prima riguarda un incarico assegnato da un giudice quindi da un'Autorità Pubblica quindi la base giuridica è un'estensione di questa. Nel caso di CTP il cliente è un privato che ci assegna una consulenza, quindi la base giuridica tipica in questo caso sarà il consenso.
Q.54.	Mi occupo di progettazione e utilizzo diversi programmi CAD. Ho sentito parlare di Protezione dei Dati fin dalla progettazione. Che cosa devo fare nelle attività di progettazione che svolgo?	**R.54.**	Il GDPR riguarda la protezione di dati personali così come definiti all'art. 4 del GDPR. *«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;* Risulta difficile che un disegno CAD contenga dati personali, pertanto è probabile che gran parte delle attività non sia nell'ambito di applicazione del GDPR. Ciò non toglie che i disegni CAD non debbano essere protetti in quanto fanno parte di una proprietà intellettuale che ha un valore, questo è ambito della sicurezza delle informazioni ma non risulta essere un obbligo di legge ma volontaria.
Q.55.	Ho uno studio professionale e condivido dei locali con un collega avvocato. Condividiamo la rete, il sistema di backup, e alcuni software di gestione amministrativa e contabile. È un problema questo per la conformità?	**R.55.**	L'ingegnere e l'avvocato (il concetto si applica a qualsiasi professionista) si configurano tendenzialmente come due Titolari autonomi fra di loro (potrebbero essere dei Contitolari nel caso di un cliente preso e su cui lavorano congiuntamente), quindi tendenzialmente l'uno non ha una base giuridica valida per vedere dati personali raccolti dall'altro. È opportuno che vengano predisposte delle misure di sicurezza atte a separare virtualmente i due studi professionali ad esempio attraverso la separazione virtuale della rete (VLAN) in due reti così come i sistemi di backup, predisporre una separazione fisica attraverso armadi chiusi a chiave separati in cui sono raccolte le pratiche, chiudere le porte, proteggere i PC con password e cifratura dei dischi.

5.5 Sezione 5: FAQ del Garante della Protezione dei dati personali

5.5.1 Sezione 5.1: FAQ Garante della Protezione dei Dati personali – Cookie

ID Q	Domanda	ID R	Risposta
Q.56.	Cosa sono i cookie[37]?	**R.56.**	I cookie sono piccoli file di testo che i siti visitati dagli utenti inviano ai loro browser, ove vengono memorizzati per essere poi ritrasmessi agli stessi siti alla visita successiva. I cookie delle c.d. "terze parti" vengono, invece, impostati da un sito web diverso da quello che l'utente sta visitando.
Q.57.	A cosa servono i cookie?	**R.57.**	I cookie sono usati per differenti finalità: esecuzione di autenticazioni informatiche, monitoraggio di sessioni, memorizzazione di informazioni su specifiche configurazioni riguardanti gli utenti che accedono al server, memorizzazione delle preferenze, ecc.
Q.58.	Cosa sono i cookie "tecnici"?	**R.58.**	Sono i cookie che servono a effettuare la navigazione o a fornire un servizio richiesto dall'utente. Non vengono utilizzati per scopi ulteriori e sono normalmente installati direttamente dal titolare del sito web. Senza il ricorso a tali cookie, alcune operazioni non potrebbero essere compiute o sarebbero più complesse e/o meno sicure, come ad esempio le attività di home banking (visualizzazione dell'estratto conto, bonifici, pagamento di bollette, ecc.), per le quali i cookie, che consentono di effettuare e mantenere l'identificazione dell'utente nell'ambito della sessione, risultano indispensabili.
Q.59.	Cosa sono i "cookie analytics"?	**R.59.**	Sono i cookie che servono a monitorare l´uso del sito da parte degli utenti per finalità di ottimizzazione dello stesso e possono essere assimilati ai cookie tecnici se realizzati e utilizzati direttamente dal sito prima parte, ovvero senza l´intervento di soggetti terzi.
Q.60.	I cookie analytics sono cookie "tecnici"?	**R.60.**	No. Il Garante (cfr. provvedimento dell´8 maggio 2014) ha precisato che possono essere assimilati ai cookie tecnici soltanto se utilizzati a fini di ottimizzazione del sito direttamente dal titolare del sito stesso, che potrà raccogliere informazioni in forma aggregata sul numero degli utenti e su come questi visitano il sito. A queste condizioni, per i cookie analytics valgono le stesse regole, in tema di informativa e consenso, previste per i cookie tecnici.
Q.61.	Cosa sono i cookie "di profilazione"?	**R.61.**	Sono i cookie utilizzati per tracciare la navigazione dell'utente in rete e creare profili sui suoi gusti, abitudini, scelte, ecc. Con questi cookie possono essere trasmessi al terminale dell'utente messaggi pubblicitari in linea con le preferenze già manifestate dallo stesso utente nella navigazione online.
Q.62.	È necessario il consenso dell'utente per l'installazione dei cookie sul suo terminale?	**R.62.**	Dipende dalle finalità per le quali i cookie vengono usati e, quindi, se sono cookie "tecnici" o di "profilazione". Per l'installazione dei cookie tecnici non è richiesto il consenso degli utenti, mentre è necessario dare l'informativa (art. 13 del Codice privacy). I cookie di profilazione, invece, possono essere installati sul terminale dell'utente soltanto se questo abbia espresso il proprio consenso dopo essere stato informato con modalità semplificate.
Q.63.	In che modo il titolare del sito deve fornire l'informativa semplificata e richiedere il consenso all'uso dei cookie di profilazione?	**R.63.**	Come stabilito dal Garante nel provvedimento indicato alla domanda n. 4, l'informativa va impostata su due livelli. Nel momento in cui l'utente accede a un sito web (sulla home page o su qualunque altra pagina), deve immediatamente comparire un banner contenente una prima informativa "breve", la richiesta di consenso all'uso dei cookie e un link per accedere ad un'informativa più "estesa". In questa pagina, l'utente potrà reperire maggiori e più

ID Q	Domanda	ID R	Risposta
			dettagliate informazioni sui cookie scegliere quali specifici cookie autorizzare.
Q.64.	Come deve essere realizzato il banner?	**R.64.**	Il banner deve avere dimensioni tali da coprire in parte il contenuto della pagina web che l'utente sta visitando. Deve poter essere eliminato soltanto tramite un intervento attivo dell'utente, ossia attraverso la selezione di un elemento contenuto nella pagina sottostante.
Q.65.	Quali indicazioni deve contenere il banner?	**R.65.**	Il banner deve specificare che il sito utilizza cookie di profilazione, eventualmente anche di "terze parti", che consentono di inviare messaggi pubblicitari in linea con le preferenze dell'utente.
Q.66.	In che modo può essere documentata l'acquisizione del consenso effettuata tramite l'uso del banner?	**R.66.**	Deve contenere il link all'informativa estesa e l'indicazione che, tramite quel link, è possibile negare il consenso all'installazione di qualunque cookie.
Q.67.	Il consenso online all'uso dei cookie può essere chiesto solo tramite l'uso del banner?	**R.67.**	Deve precisare che se l'utente sceglie di proseguire "saltando" il banner, acconsente all'uso dei cookie.
Q.68.	L'obbligo di usare il banner grava anche sui titolari di siti che utilizzano solo cookie tecnici?	**R.68.**	Per tenere traccia del consenso acquisito, il titolare del sito può avvalersi di un apposito cookie tecnico, sistema non particolarmente invasivo e che non richiede a sua volta un ulteriore consenso.
Q.69.	Cosa deve indicare l'informativa "estesa"?	**R.69.**	In presenza di tale "documentazione", non è necessario che l'informativa breve sia riproposta alla seconda visita dell'utente sul sito, ferma restando la possibilità per quest'ultimo di negare il consenso e/o modificare, in ogni momento e in maniera agevole, le proprie opzioni, ad esempio tramite accesso all'informativa estesa, che deve essere quindi linkabile da ogni pagina del sito.
Q.70.	Chi è tenuto a fornire l'informativa e a richiedere il consenso per l'uso dei cookie?	**R.70.**	No. I titolari dei siti hanno sempre la possibilità di ricorrere a modalità diverse da quella individuata dal Garante nel provvedimento sopra indicato, purché le modalità prescelte presentino tutti i requisiti di validità del consenso richiesti dalla legge.
Q.71.	L'uso dei cookie va notificato al Garante?	**R.71.**	No. In questo caso, il titolare del sito può dare l'informativa agli utenti con le modalità che ritiene più idonee, ad esempio, anche tramite l'inserimento delle relative indicazioni nella privacy policy indicata nel sito.
Q.72.	Quando entrano in vigore le misure prescritte dal Garante con il provvedimento dell'8 maggio 2014?	**R.72.**	Deve contenere tutti gli elementi previsti dalla legge, descrivere analiticamente le caratteristiche e le finalità dei cookie installati dal sito e consentire all'utente di selezionare/deselezionare i singoli cookie.

5.5.2 Sezione 5.1: FAQ Garante della Protezione dei Dati personali – Data Protectio Office[38]

ID Q	Domanda	ID R	Risposta
Q.73.	Chi è il responsabile della protezione dei dati personali (RPD) e quali sono i suoi compiti?	**R.73.**	Il responsabile della protezione dei dati personali (anche conosciuto con la dizione in lingua inglese Data Protection Officer – DPO) è una figura prevista dall'art. 37 del Regolamento (UE) 2016/679. Si tratta di un soggetto designato dal titolare o dal responsabile del trattamento per assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del Regolamento medesimo. Coopera con l'Autorità (e proprio per questo, il suo nominativo va comunicato al Garante; v. faq 6) e costituisce il punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali (artt. 38 e 39 del Regolamento).
Q.74.	Quali requisiti deve possedere il responsabile della protezione dei dati personali?	**R.74.**	Il responsabile della protezione dei dati personali, al quale non sono richieste specifiche attestazioni formali o l'iscrizione in appositi albi, deve possedere un'approfondita conoscenza della normativa e delle prassi in materia di privacy, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento. Deve poter offrire, con il grado di professionalità adeguato alla complessità del compito da svolgere, la consulenza necessaria per progettare, verificare e mantenere un sistema organizzato di gestione dei dati personali, coadiuvando il titolare nell'adozione di un complesso di misure (anche di sicurezza) e garanzie adeguate al contesto in cui è chiamato a operare. Deve inoltre agire in piena indipendenza (considerando 97 del Regolamento UE 2016/679) e autonomia, senza ricevere istruzioni e riferendo direttamente ai vertici. Il responsabile della protezione dei dati personali deve poter disporre, infine, di risorse (personale, locali, attrezzature, ecc.) necessarie per l'espletamento dei propri compiti.
Q.75.	Chi sono i soggetti privati obbligati alla sua designazione?	**R.75.**	Sono tenuti alla designazione del responsabile della protezione dei dati personali il titolare e il responsabile del trattamento che rientrino nei casi previsti dall'art. 37, par. 1, lett. b) e c), del Regolamento (UE) 2016/679. Si tratta di soggetti le cui principali attività (in primis, le attività c.d. di "core business") consistono in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala o in trattamenti su larga scala di categorie particolari di dati personali o di dati relative a condanne penali e a reati (per quanto attiene alle nozioni di "monitoraggio regolare e sistematico" e di "larga scala", v. le "Linee guida sui responsabili della protezione dei dati" del 5 aprile 2017, WP 243). Il diritto dell'Unione o degli Stati membri può prevedere ulteriori casi di designazione obbligatoria del responsabile della protezione dei dati (art. 37, par. 4). Ricorrendo i suddetti presupposti, sono tenuti alla nomina, a titolo esemplificativo e non esaustivo: istituti di credito; imprese assicurative; sistemi di informazione creditizia; società finanziarie; società di informazioni commerciali; società di revisione contabile; società di recupero crediti; istituti di vigilanza; partiti e movimenti politici; sindacati; caf e patronati; società operanti nel settore delle "utilities" (telecomunicazioni, distribuzione di energia elettrica o gas); imprese di somministrazione di lavoro e ricerca del personale; società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione; società di call center; società che forniscono servizi informatici; società che erogano servizi televisivi a pagamento.

ID Q	Domanda	ID R	Risposta
Q.76.	Chi sono i soggetti per i quali non è obbligatoria la designazione del responsabile della protezione dei dati personali?	**R.76.**	Nei casi diversi da quelli previsti dall'art. 37, par. 1, lett. b) e c), del Regolamento (UE) 2016/679, la designazione del responsabile del trattamento non è obbligatoria (ad esempio, in relazione a trattamenti effettuati da liberi professionisti operanti in forma individuale; agenti, rappresentanti e mediatori operanti non su larga scala; imprese individuali o familiari; piccole e medie imprese, con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti: v. anche considerando 97 del Regolamento, in relazione alla definizione di attività "accessoria"). In ogni caso, resta comunque raccomandata, anche alla luce del principio di "accountability" che permea il Regolamento, la designazione di tale figura (v., in proposito, le menzionate linee guida), i cui criteri di nomina, in tale evenienza, rimangono gli stessi sopra indicati.
Q.77.	È possibile nominare un unico responsabile della protezione dei dati personali nell'ambito di un gruppo imprenditoriale?	**R.77.**	Il Regolamento (UE) 2016/679 prevede che un gruppo imprenditoriale (v. definizione di cui all'art. 4, n. 19) possa designare un unico responsabile della protezione dei dati personali, purché tale responsabile sia facilmente raggiungibile da ciascuno stabilimento (sul concetto di "raggiungibilità", v. punto 2.3 delle linee guida in precedenza menzionate). Inoltre, dovrà essere in grado di comunicare in modo efficace con gli interessati e di collaborare con le autorità di controllo.
Q.78.	Il responsabile della protezione dei dati personali deve essere un soggetto interno o può essere anche un soggetto esterno? Quali sono le modalità per la sua designazione?	**R.78.**	Il ruolo di responsabile della protezione dei dati personali può essere ricoperto da un dipendente del titolare o del responsabile (non in conflitto di interessi) che conosca la realtà operativa in cui avvengono i trattamenti; l'incarico può essere anche affidato a soggetti esterni, a condizione che garantiscano l'effettivo assolvimento dei compiti che il Regolamento (UE) 2016/679 assegna a tale figura. Il responsabile della protezione dei dati scelto all'interno andrà nominato mediante specifico atto di designazione, mentre quello scelto all'esterno, che dovrà avere le medesime prerogative e tutele di quello interno, dovrà operare in base a un contratto di servizi. Tali atti, da redigere in forma scritta, dovranno indicare espressamente i compiti attribuiti, le risorse assegnate per il loro svolgimento, nonché ogni altra utile informazione in rapporto al contesto di riferimento. Nell'esecuzione dei propri compiti, il responsabile della protezione dei dati personali (interno o esterno) dovrà ricevere supporto adeguato in termini di risorse finanziarie, infrastrutturali e, ove opportuno, di personale. Il titolare o il responsabile del trattamento che abbia designato un responsabile per la protezione dei dati personali resta comunque pienamente responsabile dell'osservanza della normativa in materia di protezione dei dati e deve essere in grado di dimostrarla (art. 5, par. 2, del Regolamento; v. anche i punti 3.2 e 3.3. delle linee guida sopra richiamate). I dati di contatto del responsabile designato dovranno essere infine pubblicati dal titolare o responsabile del trattamento. Non è necessario - anche se potrebbe rappresentare una buona prassi - pubblicare anche il nominativo del responsabile della protezione dei dati: spetta al titolare o al responsabile e allo stesso responsabile della protezione dei dati, valutare se, in base alle specifiche circostanze, possa trattarsi di un'informazione utile o necessaria. Il nominativo del responsabile della protezione dei dati e i relativi dati di contatto vanno invece comunicati all'Autorità di controllo.

ID Q	Domanda	ID R	Risposta
Q.79.	Il ruolo di responsabile della protezione dei dati personali è compatibile con altri incarichi?	**R.79.**	Si, a condizione che non sia in conflitto di interessi. In tale prospettiva, appare preferibile evitare di assegnare il ruolo di responsabile della protezione dei dati personali a soggetti con incarichi di alta direzione (amministratore delegato; membro del consiglio di amministrazione; direttore generale; ecc.), ovvero nell'ambito di strutture aventi potere decisionale in ordine alle finalità e alle modalità del trattamento (direzione risorse umane, direzione marketing, direzione finanziaria, responsabile IT ecc.). Da valutare, in assenza di conflitti di interesse e in base al contesto di riferimento, l'eventuale assegnazione di tale incarico ai responsabili delle funzioni di staff (ad esempio, il responsabile della funzione legale).
Q.80.	Il responsabile della protezione dei dati personali è una persona fisica o può essere anche un soggetto diverso?	**R.80.**	Il Regolamento (UE) 2016/679 prevede espressamente che il responsabile della protezione dei dati personali possa essere un "dipendente" del titolare o del responsabile del trattamento (art. 37, par. 6, del Regolamento); ovviamente, nelle realtà organizzative di medie e grandi dimensioni, il responsabile della protezione dei dati personali, da individuarsi comunque in una persona fisica, potrà essere supportato anche da un apposito ufficio dotato delle competenze necessarie ai fini dell'assolvimento dei propri compiti. Qualora il responsabile della protezione dei dati personali sia individuato in un soggetto esterno, quest'ultimo potrà essere anche una persona giuridica (v. il punto 2.4 delle suddette Linee guida). Si raccomanda, in ogni caso, di procedere a una chiara ripartizione di competenze, individuando una sola persona fisica atta a fungere da punto di contatto con gli interessati e l'Autorità di controllo.

6. ALLEGATI

In questa sezione del documento vengono proposti alcuni modelli che l'ingegnere professionista o lo studio associato può utilizzare per alcuni degli adempimenti richiesti dalla normativa e che sono stati precedentemente indicati. Nello specifico sono riportati, sia in forma testuali che come file che possono essere personalizzati e adattati al contesto specifico, i seguenti documenti:

- Bozza dell'informativa sul trattamento dei dati personali;
- Bozza del consenso al trattamento;
- Bozza di nomina dei soggetti autorizzati al trattamento:
  - o Responsabile del Trattamento;
  - o Addetto al Trattamento;
- Modello per redigere il Registro delle attività di trattamento:
- Modello del Garante della protezione dei Dati personali per la comunicazione di Violazione dei Dati personali (Data breach).

La documentazione è proposta sotto forma di esempi che dovranno necessariamente essere adattati alle diverse situazioni ed ai diversi soggetti ai quali saranno applicati.
L'ultima parte degli allegati è infine dedicata alle Checklist di autovalutazione
In generale nei paragrafi che seguono sono evidenziate in rosso le parti di testo che sono inserite a titolo di esempio o che devono essere personalizzate o adattate dal professionista nella redazione della propria modulistica. Sono invece evidenziate in corsivo le indicazioni su come e in che modalità queste devono essere personalizzate. Queste parti di indicazioni vanno eliminate nella versione finale che verrà poi adottata dall'ingegnere professionista o dallo studio associato.

6.1 Bozza dell'informativa sul trattamento dei dati personali

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI

La presente informativa, redatta ai sensi dell'art. 13 del regolamento europeo 679/2016 (General Data Protection Regulation - di seguito GDPR), fornisce informazioni dettagliate sulla protezione dei Suoi dati personali di cui lo Studio d'Ingegneria *<nome studio/nome professionista>* (di seguito Studio) entrerà in possesso con l'affidamento dell'incarico.
In particolare, lo scopo di questo documento è di informarLa su quali Suoi dati trattiamo, le finalità per cui questi vengono trattati e condivisi, le modalità con cui vengono trattati e per quanto tempo sono conservati. Inoltre, viene indicata la base giuridica del trattamento, quali sono i Suoi diritti e come Lei potrà esercitarli. Infine, vengono riportate tutte le informazioni sul titolare del trattamento e le modalità di contatto.

Il trattamento dei dati personali da Lei forniti viene effettuato dallo Studio nel rispetto dei principi di liceità, correttezza e trasparenza e di tutela della Sua riservatezza e dei Suoi diritti, attraverso l'utilizzo di misure di sicurezza idonee ed a seguito del conferimento del Suo consenso.

Categorie dei dati trattati

Per dati personali si intendono le informazioni relative ad una persona fisica, identificata o identificabile. Per identificabile si intende la persona fisica che può essere identificata, direttamente o indirettamente, mediante riferimento ad un identificativo, come ad esempio il nome ed il cognome, il luogo e la data di nascita, l'indirizzo di residenza, il numero di telefono, l'indirizzo e-mail, ecc.
Raccogliamo e trattiamo i Suoi dati personali solo per quanto strettamente necessario alle nostre attività. In Particolare raccogliamo i seguenti dati:

- dati anagrafici (nome, cognome, documento d'identità, luogo e data di nascita, ecc.);
- informazioni di contatto (numeri di telefono, indirizzo, indirizzo di posta elettronica, ecc.);
- dati fiscali (codice fiscale, partita IVA).

Vanno inseriti i dati personali che sono raccolti con annessa la presente informativa al trattamento, vanno pertanto aggiunti dati non presenti nell'elenco precedente ed eliminati quelli che non sono raccolti.

Finalità del trattamento

I dati personali raccolti vengono trattati dallo Studio, ai sensi del GDPR, in forza dell'affidamento dell'incarico professionale e/o sulla base del Suo esplicito consenso per finalità accessorie all'erogazione dei servizi descritti:

- eseguire il contratto o le misure precontrattuali;
- adempiere agli obblighi fiscali e contabili;
- rispettare gli obblighi gravanti sul professionista, previsti dal GDPR e dalla normativa vigente in materia di protezione dei dati personali;
- invio e-mail per convegni o newsletter per attività di comunicazione;
- la Sua registrazione ai servizi offerti dallo Studio attraverso il suo sito internet www.<xxxxxxxxxxxxxxxxxxxx>, nei limiti di quanto strettamente necessario alla fornitura dei servizi stessi.

Base giuridica del trattamento

Il conferimento dei Suoi dati personali è obbligatorio per tutto ciò che è richiesto dagli obblighi legali e contrattuali e pertanto l'eventuale rifiuto a comunicarli, in tutto o in parte, impedisce di fornire la prestazione richiesta.
I Suoi dati personali sono trattati lecitamente dallo Studio per:

- eseguire un contratto di cui Lei è parte o per eseguire misure precontrattuali;

- adempiere ad obblighi di legge, regolamenti ed ordini delle Autorità;
- trattamenti specifici che richiedono il Suo consenso quali invio di e-mail o di newsletter per inviti e comunicazioni varie.

Modalità del trattamento
Il trattamento dei dati personali è effettuato sia con supporti cartacei che con strumenti automatizzati atti a memorizzare, gestire e trasmettere i dati stessi. Sono osservate idonee misure di sicurezza per prevenire la perdita dei dati, gli usi illeciti o non corretti e gli accessi non autorizzati.

Soggetti cui possono venire comunicati i dati personali
Lo Studio non fornisce a soggetti terzi i Suoi dati personali senza il Suo preventivo consenso, salvo ove richiesto dalla legge o per l'esecuzione dell'incarico professionale affidato.
Nella gestione dei Suoi dati personali, potranno venire a conoscenza degli stessi i dipendenti e/o i collaboratori dello Studio, che operano in qualità di autorizzati al trattamento dei Suoi dati personali, nominati per iscritto, opereranno con apposite istruzioni e saranno debitamente formati per garantire la tutela dei dati del cliente.
I Suoi dati personali potranno inoltre essere comunicati, a consulenti fiscali esterni per l'adempimento degli obblighi fiscali e contabili; società di assistenza informatica o collaboratori che elaborano i dati; istituti bancari per la gestione degli incassi e dei pagamenti; autorità di vigilanza e controllo.

Periodo di conservazione dei dati personali
Tutti i dati personali acquisiti dallo Studio saranno conservati per il tempo strettamente necessario all'esecuzione dell'incarico e, in seguito, per il periodo obbligatorio di conservazione delle scritture contabili.

Diritti dell'interessato
Lei avrà la facoltà di esercitare, in qualsiasi momento, i diritti previsti dal GDPR, tra cui:

- il diritto di chiedere al professionista **l'accesso** ai Suoi dati personali ed una copia degli stessi;
- la **rettifica**, dei Suoi dati personali, mediante integrazione o correzione, qualora ritenga che gli stessi siano inesatti, non aggiornati o incompleti;
- la **cancellazione** dei Suoi dati personali, se sussistono i motivi previsti dalla legge;
- la **limitazione** del trattamento dei dati personali che La riguardano;
- **l'opposizione** al trattamento dei Suoi dati personali per motivi relativi alla Sua particolare situazione;
- il diritto alla **portabilità** dei Suoi dati personali mediante trasmissione diretta, se tecnicamente possibile, ad altro titolare;
- la **revoca** al consenso che ha prestato senza che ciò pregiudichi la liceità del trattamento basata sul consenso da Lei prestato prima della revoca;
- il diritto di proporre **reclamo** al Garante, come previsto dall'art. 77 del Regolamento stesso, o di adire le opportune sedi giudiziarie (art. 79 del Regolamento). I dati di contatto del Garante per la protezione dei dati personali sono:
  Centralino telefonico: (+39) 06.696771

  Fax: (+39) 06.69677.3785
  E-mail: garante@gpdp.it
  Posta certificata: protocollo@pec.gpdp.it
  Sito istituzionale: www.garanteprivacy.it

Titolare del trattamento
Il titolare del trattamento dei Suoi dati personali è lo Studio <xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> che può essere contattato tramite:

- e-mail:<xxxxxxxxxxxxxxx>@<xxxxxxxxxx>
- PEC:<xxxxxxxxxxxxxxxxx>@<xxxxxxxxxx>
- Tel.: <xxxxxxxxxxxxxxxxx>

(In caso di Studio associato, indicare i riferimenti del legale rappresentante)
(Se lo Studio ha nominato un responsabile della protezione dei dati personali RPD ovvero, Data Protectio Officier DPO, indicare anche i suoi dati di contatto).

Guides

FAQ

Support

CONSENSO AL TRATTAMENTO

Il/La sottoscritto/a _____ presa visione dell'informativa rilasciata ai sensi dell'art. 13 del GDPR,

☐ presta il consenso ☐ nega il consenso

al trattamento da parte dello Studio dei propri dati personali per le attività sopra descritte per le quali il consenso rappresenti la base giuridica del trattamento.

(Luogo, data)

_____

(Firma)

_____

6.2 Bozza Consenso al Trattamento dei dati personali

6.3 Bozza di lettera di nomina dei soggetti individuati

Lettera di incarico a Responsabile del trattamento dei dati personali ai sensi del Regolamento n. 2016/679 del Parlamento Europeo

Lo Studio <nome studio> con sede legale in <luogo studio ed indirizzo> P. IVA <numero partita IVA> , nella persona del <titolo nome cognome> in qualità di Titolare del trattamento dei dati personali,

- visto il Regolamento n. 2016/679 del Parlamento Europeo, in vigore dal 25 maggio 2018, (di seguito definito "Regolamento"), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (RGPD: Regolamento Generale sulla Protezione dei Dati, meglio noto con la sigla inglese GDPR: General Data Protection Regulation),
- visto l'art. 4 paragrafo 8 del Regolamento che definisce come 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",
- considerato che l'art. 28 paragrafo 1 del Regolamento stabilisce che "Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che prestino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato",
- considerato che l'art. 28 paragrafo 2 del Regolamento dispone che "Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento",
- considerato che l'art. 28 paragrafo 3 del Regolamento dispone che "I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la

finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento",
- considerato che l'art 28 paragrafo 4 del Regolamento dispone che "Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento",
- preso atto che l'art. 29 del Regolamento stabilisce che "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",

nomina

<persona fisica / persona giuridica>, nella persona del *<titolo nome cognome>*, legale rappresentante della stessa (specificazione necessaria solo nel caso di persone giuridiche)

Responsabile del trattamento dei dati personali relativamente e limitatamente ai trattamenti effettuati per conto dello Studio con qualsiasi strumento (elettronico e non) e riguardanti i seguenti servizi:
<elenco servizi>

Con riferimento a tale nomina, il *Responsabile* del trattamento dovrà:

- trattare i dati personali soltanto su istruzione documentata del Titolare del trattamento;
- rispettare i principi di liceità, correttezza e trasparenza, osservando il Regolamento e gli altri regolamenti e leggi in materia di riservatezza dei dati personali;
- trattare i dati solo in relazione all'attività che viene svolta e conservarli per un periodo non superiore a quello necessario per gli scopi del trattamento;
- aggiornare periodicamente l'elenco dei trattamenti dei dati personali e le relative banche dati gestite dallo studio, tenere un registro, in formato elettronico, di tutte le categorie di attività relative al trattamento, svolte per conto del Titolare, come previsto dall'art. 30 del Regolamento;
- nominare per iscritto gli Autorizzati al trattamento e garantire che si impegnino alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- fornire le istruzioni operative agli Autorizzati al trattamento, anche sotto il profilo delle misure di sicurezza;
- adottare tutte le misure richieste ai sensi dell'art. 32 del Regolamento mettendo in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio;
- rispettare le condizioni di cui ai paragrafi 2 e 4 dell'art 28 del Regolamento per ricorrere a un altro Responsabile del trattamento;
- assistere il Titolare del trattamento, con misure tecniche ed organizzative adeguate, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III del Regolamento;
- informare il Titolare del trattamento, senza ingiustificato ritardo e comunque entro 72 ore, dopo essere venuto a conoscenza di una violazione dei dati personali (data breach) ed adottare, insieme allo stesso, nuove misure di sicurezza atte a limitare gli effetti negativi dell'evento ed a ripristinare la situazione precedente;
- assistere il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli artt. 35 e 36 del Regolamento;
- su scelta del Titolare del trattamento, cancellare o restituire tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;
- mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi stabiliti dal Regolamento e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato;
- informare immediatamente il Titolare del trattamento qualora, a suo parere, un'istruzione violi il Regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati;
- trattare i dati con la massima riservatezza ed impedirne, per quanto possibile, l'accesso a persone non autorizzate;
- predisporre un sistema di sicurezza idoneo a rispettare le disposizioni previste dal Regolamento e da ogni altra disposizione in materia ed adeguare tale sistema alle norme future in materia di sicurezza.

Quanto sopra costituisce un'indicazione esemplificativa dei compiti assegnati ai fini dell'esecuzione dell'accordo. Ulteriori istruzioni potranno, di volta in volta, essere fornite dal Titolare del trattamento, qualora lo stesso ne ravvisasse la necessità.
Per ogni altra misura ed istruzione qui non prevista, si rimanda al Regolamento che viene allegato alla presente.
Si ricorda che l'inosservanza delle presenti istruzioni può comportare sanzioni anche di natura penale.
La presente nomina decorre dalla data in cui viene sottoscritta dalle Parti ed è valida fino alla cessazione delle attività sopra descritte, salvo revoca anticipata, per qualsiasi motivo, da parte

Il Titolare

Il Responsabile per accettazione

6.4 Bozza del registro dei trattamenti

REGISTRO ATTIVITA' DI TRATTAMENTO (art.30, c.1, GDPR)			
TITOLARE DEL TRATTAMENTO		**DATA PROTECTION OFFICER**	
Indirizzo		Indirizzo	
N. Telefono		N. Telefono	
Mail		Mail	
PEC		PEC	
DELEGATO/RAPPRESENTANTE DAL TITOLARE (eventuale)		**Registro Tenuto Da**	
Indirizzo		Data Creazione	
N. Telefono		Ultimo Aggiornamento	
Mail		N. Schede Compilate	
PEC		Prossima Revisione	

	TRATTAMENTO			DATI PERSONALI			INTERESSATI		DESTINATARI		TRASFERIMENTI	SICUREZZA
n. ordine	Descrizione	Finalità	Contitolare (eventuale rappresentante)	Categoria	Dati Particolari (ex sensibili) SI/NO	Termine Ultimo Cancellazione	Categoria	Consenso (SI/NO)	Categoria	Paesei terzi, org.ni int.li (eventuale) SI/NO	Paesei terzi, org.ni int.li (eventuale) SI/NO	Misure Tecniche ed organizzative adottate (e rimandi ad eventuali allegati di dettaglio

Figura 3

REGISTRO CATEGORIE DI ATTIVITA' DI TRATTAMENTO (art.30, c.2, GDPR)			
TITOLARE DEL TRATTAMENTO		**RESPONSABILE DEL TRATTAMENTO**	
Indirizzo		Indirizzo	
N. Telefono		N. Telefono	
Mail		Mail	
PEC		PEC	
DELEGATO/RAPPRESENTANTE DAL TITOLARE (eventuale)		**DATA PROTECTION OFFICER**	
Indirizzo		Indirizzo	
N. Telefono		N. Telefono	
Mail		Mail	
PEC		PEC	
		Registro Tenuto Da	
		Data Creazione	
		Ultimo Aggiornamento	
		N. Schede Compilate	
		Prossima Revisione	

	TRATTAMENTO			TRASFERIMENTI	SICUREZZA
n. ordine	Descrizione	Finalità	Contitolare	Paesei terzi, org.ni	Misure Tecniche ed

Figura 4

del Titolare del trattamento.
<luogo>, <data>

6.5 Template Data Breach

Per la notifica al Garante Privacy di un data breach si faccia riferimento al modello pubblicato sul sito dell'Authority:
https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9128501

6.6 Checklist di autovalutazione

6.6.1 Legittimità, correttezza e trasparenza

Informazioni in tuo possesso

- **Il tuo Studio ha effettuato un controllo delle informazioni per ottenere una mappa dei flussi di dati (elenco dei trattamenti)?**

È necessario organizzare una verifica delle informazioni che lo Studio raccoglie e utilizza per le sue attività. Questa ricerca serve ad identificare i dati personali e particolari (ex sensibili) che sono elaborati e le modalità nelle quali questi flussi di informazioni vengono raccolti, trattati, ed eventualmente ceduti o esposti, attraverso e fuori dalla vostra attività di business.
Un flusso di informazioni può includere un trasferimento di informazioni da una posizione a un'altra, all'interno dello Studio, o un trasferimento ad altro ufficio che si trova altrove (fuori sede).

- **Il tuo Studio ha documentato quali dati personali raccoglie, come li raccoglie, con chi li condivide e come li utilizza?**

Dopo la verifica delle informazioni, è necessario documentare i risultati in un Registro dei trattamenti.
Per rispettare il principio di responsabilità del GDPR, lo Studio deve essere in grado di dimostrare le modalità adottate per essere conforme ai principi del GDPR, ad esempio definendo ed applicando procedure ed istruendo il personale.
Per questo motivo, è necessario riportare in un documento:

- il nome e i dettagli dell'attività, il legale rappresentante e il responsabile della protezione dei dati (DPO);
- le finalità dei trattamenti;
- le categorie di interessati e quelle dei dati personali trattati;
- i tempi di conservazione dei dati personali;
- i dettagli di eventuali trasferimenti verso paesi terzi, compresa la documentazione delle garanzie del meccanismo di trasferimento in vigore, se applicabile;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

È necessario conservare queste informazioni (Registro dei trattamenti) per tutte le attività che:

- non sono occasionali;
- potrebbero comportare un rischio per i diritti e le libertà delle persone; o
- comportano il trattamento di particolari categorie di dati o di condanne penali e dati di reato.

Queste informazioni dovrebbero essere disponibili su richiesta dell'Autorità di Controllo.

Base legale per il trattamento dei dati personali

- **Il tuo Studio ha identificato le basi legali per l'elaborazione di dati personali e le ha documentate?**

È necessario identificare i principi legali alla base del trattamento dei dati personali prima di poterli richiedere ed elaborare.
L'elaborazione si basa su sei principi di legittimità su cui si fonda lo scopo del trattamento e del rapporto con l'individuo.
In breve, i sei principi sono:

1) **Consenso:** l'individuo ha fornito un chiaro

consenso al trattamento dei propri dati personali per uno scopo specifico;

2) **Contratto:** il trattamento è necessario per adempiere ad un contratto stipulato con l'individuo o perché necessario per l'adozione di provvedimenti specifici prima di stipulare un atto legale;
3) **Obbligo legale:** il trattamento è necessario per il rispetto della legge (non compresi gli obblighi contrattuali);
4) **Interessi vitali:** il trattamento è necessario per proteggere la vita di qualcuno;
5) **Compito pubblico:** l'attività o la funzione ha una base giuridica chiara e l'elaborazione è necessaria per l'esecuzione di un compito nel pubblico interesse o per le funzioni ufficiali;
6) **Interessi legittimi:** il trattamento è necessario per gli interessi legittimi del tuo Studio o di terzi, a meno che non vi siano buone ragioni per proteggere i dati personali dell'individuo che superano tali interessi legittimi. (Questo non può essere applicato alle autorità pubbliche nell'elaborazione di dati in esecuzione delle loro attività ufficiali.)

Qualora si stiano elaborando dati di categorie speciali o dati di reato, è necessario identificare sia una base legale per l'elaborazione generale che una condizione aggiuntiva (condizione dell'articolo 9) per l'elaborazione di questo tipo di dati. È necessario fornire agli interessati, informazioni su come si intendono trattare i loro dati personali e quale base legale è prevista.

Consenso

- **Il tuo Studio ha adeguato le modalità di richiesta e registrazione del consenso?**

La richiesta di consenso deve offrire alle per-

sone (gli interessati) una scelta e un controllo genuini sulle modalità di utilizzo dei loro dati, al fine di creare fiducia e migliorare la reputazione aziendale.
La richiesta di consenso si basa sui seguenti requisiti:

- deve mettere in evidenza la/le richiesta/e di consenso e separarla da altre indicazioni, ad es. termini e condizioni;
- deve permettere una scelta libera senza preselezioni e soprattutto esplicita (opt-in);
- deve evitare di rendere il consenso una precondizione obbligatoria della fornitura del servizio, eccetto il caso di necessità per adempiere agli obblighi contrattuali di fornitura (p.es.: se non ho i dati personali non posso stipulare un contratto di fornitura servizi);
- deve essere specifico e granulare così da consentire alle persone di acconsentire separatamente a diversi scopi e tipi di trattamento, laddove appropriato;
- deve riportare il nome del tuo Studio e delle eventuali organizzazioni (cd. terze parti) che questo consenso autorizzerà a trattare i dati personali;
- deve essere mantenuta traccia di ciò a cui una persona ha acconsentito, di quando e come ha manifestato liberamente il suo consenso;
- deve informare le persone sulle modalità "semplici" di revoca del consenso e su come attuarle in qualsiasi momento.

- **Il tuo Studio aggiorna il consenso se cambiano le modalità di trattamento o gli scopi per i quali è stato richiesto?**

Gli obblighi non finiscono con l'ottenimento del primo consenso. Non è una conformità "una tantum" che va richiesta e poi archiviata.
Il consenso deve essere aggiornato se cambia qualcosa negli scopi e modalità di trattamento che sono stati esposti nell'informativa. In questi casi o se i dati vengono trattati per altre finalità è necessario ottenere un nuovo consenso conforme a GDPR e identificare i requisiti appropriati per il trattamento che si vuole effettuare. Altrimenti bisogna interrompere l'elaborazione (cioè il trattamento) perché è illegale in quanto non sono rispettati i presupposti legali.

Consenso al trattamento dei dati personali dei minori per i servizi online

- **Se il tuo Studio offre servizi online direttamente ai minori, sono disponibili sistemi per la gestione dei consensi?**

Solo un individuo di età pari o superiore a 14 anni sarà in grado di fornire autonomamente il proprio consenso per usufruire di *"servizi offerti dalla società dell'informazione"*.
Per i minori di 14 anni è opportuno definire e descrivere una procedura utilizzata per verificare l'età, con ogni ragionevole sforzo. Parimenti, una procedura deve essere definita ed applicata per verificare che la persona che dà il consenso abbia effettivamente la responsabilità genitoriale per il minore.
È infatti necessario ottenere il consenso del trattamento dei dati personali per i minori di anni 14, da chiunque ne abbia la responsabilità genitoriale.
Negli altri casi le modalità di richiesta del consenso rimangono immutate, cioè al di sotto dei 18 anni il consenso è fornito da chi ha la responsabilità genitoriale.

Interessi vitali

- **Nell'eventualità di elaborare i dati per proteggere gli interessi vitali di un individuo, il tuo Studio ha documentato in modo chiaro le circostanze in cui questi interessi saranno rilevanti e ne ha informato le persone se necessario?**

La base legale degli interessi vitali è molto limitata nella sua portata, ed è generalmente applicabile solo alle questioni di vita e di morte. È particolarmente rilevante per le cure mediche di emergenza, quando è necessario elaborare i dati personali per scopi medici e probabilmente quando l'individuo non è in grado di dare il consenso al trattamento. Pare poco appropriato per le cure mediche pianificate in anticipo o per l'elaborazione su scala più ampia.

Interessi legittimi

- **Quando l'elaborazione dei dati personali è effettuata per legittimi interessi, il tuo Studio può dimostrare di aver pienamente considerato e protetto i diritti e gli interessi dell'individuo?**

L'identificazione della legittimità degli interessi legittimi costituisce la base legale più flessibile per l'elaborazione, ma non si può presumere che sarà sempre la più appropriata.
Il Regolamento menziona specificamente l'uso di dati di clienti o dipendenti, marketing, prevenzione di frodi, trasferimenti all'interno di un gruppo o sicurezza IT come potenziali interessi legittimi, ma questo elenco non è esaustivo.
Se si desidera fare affidamento su interessi legittimi è necessario che questi siano identificati. Bisogna quindi prendere in considerazione:

- perché si vogliono elaborare i dati - cosa si sta cercando di ottenere?
- chi trae beneficio dall'elaborazione? in quale modo?
- ci sono benefici pubblici più ampi per l'ela-

borazione?
- quanto sono importanti questi benefici?
- quale sarebbe l'impatto se non fosse possibile andare avanti?
- l'utilizzo dei dati sarà immorale o illegale in alcun modo?

6.6.2 Diritti degli individui

Diritto di essere informato, comprese le informazioni sulla privacy

- **Il tuo Studio ha fornito informazioni sulla privacy alle persone?**

Le persone, i clienti, devono sapere che si raccolgono i loro dati, per quale motivo vengono elaborati e con chi sono eventualmente condivisi.
Queste informazioni sulla privacy dovrebbero essere pubblicate sul sito web del tuo Studio e questi riferimenti riportati in qualsiasi modulo o lettera inviata alle persone. L'informazione deve essere:
- sintetica, trasparente, intelligibile e facilmente accessibile;
- scritta in un linguaggio chiaro e comprensibile, specie se rivolta a minori;
- gratuita.

Le informazioni da fornire agli interessati dipendono dalle modalità di ottenimento dei dati personali: se sono stati forniti direttamente dall'interessato o pervenuti da una terza parte.

Comunicare il trattamento dei dati personali dei minori

- **Se il tuo Studio offre servizi online direttamente ai minori, le informazioni sulla privacy vengono comunicate in modo comprensibile per il minore?**

È necessario fornire ai minori (<14 anni) le stesse informazioni sulla privacy fornite agli adulti. È buona norma spiegare anche i rischi connessi all'elaborazione e le garanzie che il tuo Studio ha messo in atto.
Qualsiasi informazione diretta ai minori dovrebbe essere concisa, chiara e scritta in un linguaggio semplice in modo che siano in grado di capire cosa accadrà ai loro dati personali e quali sono i diritti che loro hanno. Dovrebbe essere usato un linguaggio adatto all'età e presentato in un modo opportuno per un pubblico giovane.

Diritto di accesso

- **Il tuo Studio ha un processo per riconoscere e rispondere alle richieste individuali di accedere ai propri dati personali?**

Le persone hanno il diritto di ottenere:
- la conferma che il tuo Studio sta elaborando i loro dati;
- l'accesso ai propri dati personali;
- altre informazioni supplementari, generalmente riportate nelle note sulla privacy.

La richiesta delle informazioni può essere fatta verbalmente o per iscritto. È necessario fornire una copia delle informazioni gratuitamente, ma è possibile addebitare un "importo ragionevole basato sul costo amministrativo" se una richiesta è:
- manifestamente infondata o eccessiva, in particolare se è ripetitiva;
- per ulteriori copie di informazioni già fornite in precedenza.

Le informazioni devono essere fornite senza indugio e almeno entro un mese solare dal ricevimento della richiesta. Si può estendere il periodo di altri due mesi nel caso di richieste complesse o numerose (previa informazione al richiedente con spiegazioni sul ritardo). L'identità del richiedente deve essere verificata utilizzando "mezzi ragionevoli".
Se la richiesta viene effettuata elettronicamente, è necessario fornire le informazioni in un formato elettronico intellegibile e comunemente utilizzato.

Diritto di rettifica e qualità dei dati

- **Il tuo Studio ha processi per garantire che i dati personali in tuo possesso rimangano corretti e aggiornati?**

Gli interessati hanno il diritto di completare i propri dati personali o rettificarli se inesatti o incompleti.
Le richieste di rettifica possono essere presentate verbalmente o per iscritto.
È necessario rispondere a una richiesta senza indugio e almeno entro un mese dal ricevimento. Si può estendere il periodo di altri due mesi nel caso di richieste complesse o numerose (previa informazione al richiedente con spiegazioni sul ritardo). È opportuno mantenere traccia della richiesta, nonché verificare l'identità del soggetto che la effettua, utilizzando "mezzi ragionevoli".
Se i dati personali sono stati condivisi con altre organizzazioni (ad esempio altri controllori o processori), è necessario che siano informati della rettifica affinché agiscano di conseguenza.
Potrebbe essere opportuno effettuare periodici controlli sulla qualità e completezza dei dati raccolti, attivando se necessario campagne di sensibilizzazione e formazione interna.

Diritto di cancellazione inclusa la conservazione e lo smaltimento

- **Il tuo Studio ha descritto ed applica una procedura per cancellare in modo sicuro i dati personali che non sono più necessari o quelli di una persona che ne ha richiesto l'eliminazione?**

Gli interessati hanno diritto all'oblio e possono richiedere la cancellazione dei propri dati personali quando:
- non sono più necessari per gli scopi per i quali sono stati originariamente raccolti ed elaborati;

- la persona (l'interessato) ritira il consenso;
- non sono più validi gli interessi legittimi che giustificavano la raccolta dei dati personali;
- l'interessato ha sollevato obiezioni al trattamento dei propri dati personali per scopi di marketing diretto;
- i dati personali sono stati elaborati in modo illegale (cioè in violazione del Regolamento);
- serve per rispettare un obbligo legale;
- sono elaborati per servizi informatici indirizzati ad un minore.

Gli interessati possono fare una richiesta di cancellazione sia verbalmente che per iscritto. È opportuno mantenere traccia della richiesta, nonché verificare l'identità del soggetto che la effettua, utilizzando "mezzi ragionevoli".
È necessario rispondere alla richiesta senza indugio e almeno entro un mese dal ricevimento. Si può estendere il periodo di altri due mesi nel caso di richieste complesse o numerose (previa informazione al richiedente con spiegazioni sul ritardo).
Se i dati personali sono stati condivisi con altre organizzazioni (ad esempio altri controllori o processori), è necessario che siano informati della richiesta di cancellazione affinché agiscano di conseguenza.
La richiesta di cancellazione può essere rifiutata se i dati personali sono elaborati per uno dei seguenti motivi:

- esercitare il diritto alla libertà di espressione e informazione;
- rispettare un obbligo legale;
- svolgere un compito di interesse pubblico o esercitare l'autorità ufficiale;
- scopi di archiviazione nell'interesse pubblico, ricerca storica di ricerca scientifica o scopi statistici;
- esercitare o difendere un diritto in sede giudiziaria;
- scopi di pubblica sanità nell'interesse pubblico;
- trattamenti necessari ai fini della prevenzione o della medicina del lavoro.

È opportuno definire ed applicare una procedura scritta di conservazione (e cancellazione) che indichi le regole di cancellazione per le varie categorie di dati e ne pianifichi uno smaltimento sicuro. Dovrebbero essere anche definite le responsabilità delle persone cui è devoluta la conservazione e la cancellazione.

Diritto di limitare l'elaborazione

- **Il tuo Studio ha procedure per rispondere alla richiesta di una persona di limitare il trattamento dei suoi dati personali?**

Gli interessati hanno il diritto di bloccare o limitare il trattamento dei loro dati personali. La richiesta può essere presentata verbalmente o per iscritto. È opportuno mantenere traccia della richiesta, nonché verificare l'identità del soggetto che la effettua, utilizzando "mezzi ragionevoli".
È necessario rispondere alla richiesta senza indugio e almeno entro un mese dal ricevimento. Si può estendere il periodo di altri due mesi nel caso di richieste complesse o numerose (previa informazione al richiedente con spiegazioni sul ritardo).
Se i dati personali sono stati condivisi con altre organizzazioni (ad esempio altri controllori o processori), è necessario che siano informati della richiesta di blocco o limitazione del trattamento affinché agiscano di conseguenza.
Se il trattamento viene limitato, è consentito archiviare i dati personali, ma non elaborarli ulteriormente. È possibile conservare sufficienti informazioni sull'individuo per garantire che la restrizione venga rispettata in futuro.
È opportuno limitare il trattamento dei dati personali quando:

- un individuo contesta l'accuratezza dei dati personali fino a che non è stata verificata l'esattezza;
- una persona si è opposta al trattamento e si sta valutando se i motivi legittimi della raccolta prevalgono su quelli dell'interessato;
- l'elaborazione è illegale e l'interessato richiede invece una restrizione, ma non vuole la cancellazione;
- non c'è più la necessità dei dati personali, ma l'interessato richiede che i dati vengano conservati per consentirgli di stabilire, esercitare o difendere un diritto in sede giudiziaria.

Diritto alla portabilità dei dati

- **Il tuo Studio ha processi che consentono, su richiesta dell'interessato, di spostare, copiare o trasferire i suoi dati personali verso un'altra azienda, in modo sicuro, protetto e senza ostacoli all'usabilità?**

Il diritto alla portabilità dei dati consente alle persone di ottenere e riutilizzare i propri dati personali per i propri scopi presso un diverso fornitore di servizi, spostando, copiando, o trasferendo facilmente i dati in modo sicuro e protetto da un'azienda all'altra.
È necessario fornire i dati personali dell'interessato gratuitamente, in un formato strutturato, comunemente utilizzato e leggibile da una macchina, quali ad esempio i file CSV e XML. Se richiesto, potrebbero essere trasmessi direttamente a un'altra azienda se tecnicamente fattibile.
Il diritto alla portabilità dei dati si applica solo:

- ai dati personali che un interessato ha fornito a un titolare del trattamento;
- se il trattamento è basato sul consenso dell'interessato o per l'esecuzione di un contratto;
- e quando il trattamento è effettuato con mezzi automatizzati.

La richiesta può essere presentata verbalmente o per iscritto. È opportuno mantenere traccia della richiesta, nonché verificare l'identità del soggetto che la effettua, utilizzando "mezzi ragionevoli".
È necessario rispondere alla richiesta senza indugio e almeno entro un mese dal ricevimento. Si può estendere il periodo di altri due mesi nel caso di richieste complesse o numerose (previa informazione al richiedente con spiegazioni sul ritardo).

Diritto di opporsi

- **Il tuo Studio ha procedure per gestire l'opposizione di una persona al trattamento dei propri dati personali?**

Le persone hanno il diritto di opporsi al trattamento dei loro dati personali in determinate circostanze. È necessario informare in modo semplice e separatamente dalle informazioni sugli altri diritti, al momento della raccolta dei dati personali.
La richiesta può essere presentata verbalmente o per iscritto. È opportuno mantenere traccia della richiesta, nonché verificare l'identità del soggetto che la effettua, utilizzando "mezzi ragionevoli".
È necessario rispondere alla richiesta senza indugio e almeno entro un mese dal ricevimento. Si può estendere il periodo di altri due mesi nel caso di richieste complesse o numerose (previa informazione al richiedente con spiegazioni sul ritardo).
Se i dati personali sono stati condivisi con altre organizzazioni (ad esempio altri controllori o processori), è necessario che siano informati della richiesta di blocco o limitazione del trattamento affinché agiscano di conseguenza.
Gli interessati hanno il diritto assoluto di opporsi a qualsiasi elaborazione intrapresa ai fini del marketing diretto (inclusa la profilazione), che va interrotta subito non appena si riceve un'obiezione. Non ci sono esenzioni o motivi per rifiutare a meno che:

- si possano dimostrare motivi preminenti e legittimi per il trattamento che superano gli interessi, i diritti e le libertà degli individui;
- il trattamento è finalizzato alla costituzione, esercizio o difesa di un diritto in sede giudiziaria;
- il trattamento è necessario per l'esecuzione di un'attività svolta per motivi di interesse pubblico;
- il trattamento è a fini di ricerca scientifica/storica o a fini statistici.

Diritti relativi al processo decisionale automatizzato, inclusa la profilazione

- **Il tuo Studio effettua elaborazioni dei dati personali, inclusa la profilazione, che costituiscono un processo decisionale automatizzato?**

Il Regolamento fornisce garanzie contro il rischio che una decisione potenzialmente dannosa sia presa senza l'intervento umano.
Le persone hanno il diritto di non essere soggette a una decisione quando questa:

- si basa esclusivamente sull'elaborazione automatica, inclusa la profilazione; e
- produce un effetto legale o un effetto altrettanto significativo sull'individuo.

Puoi eseguire questo tipo di elaborazione solo se la decisione è:

- necessaria per stipulare o eseguire un contratto tra il tuo Studio e la persona;
- autorizzata dalla legge (ad esempio a fini di frode o di evasione fiscale); o
- in base al consenso esplicito della persona.
- Se una di queste eccezioni si concretizza, è necessario attivare misure opportune per salvaguardare i diritti dell'individuo, le libertà e i legittimi interessi. Queste misure devono includere almeno i diritti degli individui a:
- ottenere l'intervento umano;
- esprimere il loro punto di vista;
- ottenere una spiegazione delle decisioni.

La richiesta può essere presentata verbalmente o per iscritto. È opportuno mantenere traccia della richiesta, nonché verificare l'identità del soggetto che la effettua, utilizzando "mezzi ragionevoli".
È necessario rispondere alla richiesta senza indugio e almeno entro un mese dal ricevimento. Si può estendere il periodo di altri due mesi nel caso di richieste complesse o numerose (previa informazione al richiedente con spiegazioni sul ritardo).
Il Regolamento definisce la profilazione come una qualsiasi forma di elaborazione automatica intesa a valutare determinati aspetti personali di un individuo, al fine di analizzare o prevedere:

- prestazioni lavorative;
- situazione economica;
- salute;
- preferenze personali;
- affidabilità;
- comportamento;
- posizione;
- movimenti.

Sono più limitate le eccezioni disponibili per giustificare la profilazione che utilizza categorie speciali di dati personali. L'elaborazione può avvenire solo se:

- è stato ottenuto il consenso esplicito del soggetto; o
- il trattamento è necessario per motivi di reale interesse pubblico.

Ancor più delicata e preferibilmente da evitare è la profilazione o decisone automatica sui minori.

6.6.3 Responsabilità e governance

Responsabilità

- **Il tuo Studio ha una politica di protezione**

dei dati appropriata?

Il Regolamento richiede di dimostrare come i suoi princìpi sono messi in pratica.
Un documento di policy della protezione dei dati spiega come il tuo Studio affronta il problema in modo coerente e ne dimostra la responsabilità ai sensi del Regolamento.
È preferibile che la policy sia definita come un documento a se stante anche se, in aziende poco complesse potrebbe essere incluso in un documento organizzativo generale. In ogni caso la politica dovrebbe definire chiaramente l'approccio aziendale alla protezione dei dati insieme alle responsabilità per l'attuazione della politica, la loro assegnazione alle persone di riferimento e il monitoraggio della conformità.
La policy dovrebbe essere approvata dalla direzione che provvede a pubblicarla e comunicarla a tutto il personale. È necessario rivedere e aggiornare periodicamente la policy per garantirne la pertinenza agli eventuali mutamenti di scenario.

- **Il tuo Studio controlla la sua conformità con le politiche di protezione dei dati e rivede con regolarità l'efficacia della gestione dei dati e dei controlli di sicurezza?**

Emanare una policy di protezione dei dati personali, e diffonderne la conoscenza nel tuo Studio, non è sufficiente a garantire che il personale rispetti tutti i processi da esso definiti.
È opportuno predisporre una procedura che effettui la verifica della conformità dell'attuazione delle politiche di protezione e sicurezza dei dati.
Questa verifica dovrebbe essere fatta periodicamente testando le misure di protezione descritte nella policy per fornire assicurazioni sulla loro continua efficacia. L'imparzialità dei giudizi di verifica dovrebbe essere garantita da persone terze al tuo Studio o personale aziendale non coinvolto nella definizione ed attuazione della politica aziendale.

- **Il tuo Studio effettua la formazione di tutto il personale sulla sensibilizzazione alla protezione dei dati?**

Un punto fondamentale dell'attuazione del Regolamento è l'informazione di tutto il personale che tratta i dati personali sulle loro responsabilità in materia di protezione dei dati. È opportuno fornire questa formazione anche a intervalli regolari o quando richiesto dalle modifiche del contesto aziendale o delle normative vigenti.
Personale con compiti specifici, come la sicurezza delle informazioni e la gestione del database e il marketing, necessita di formazione specialistica sui temi di competenza.

Contratti di lavorazione

- **Il tuo Studio trasferisce i dati personali per le elaborazioni a fornitori esterni sulla base di contratti scritti?**

Ogni volta che si utilizza un fornitore per trattamento dei dati personali è necessario che il rapporto sia gestito da un contratto scritto o altro atto legale.
Il contratto tra le parti è richiesto dal Regolamento affinché siano definiti precisamente ruoli, responsabilità e modalità di effettuazione del lavoro da parte di entrambi. Il Regolamento stabilisce ciò che è necessario includere nel contratto.
Il tuo Studio che raccoglie i dati personali dei clienti è il Titolare del trattamento, è direttamente responsabile della conformità complessiva al Regolamento e deve dimostrare tale conformità. Se ciò non è possibile il tuo Studio può essere soggetto al pagamento di sanzioni economiche.
È necessario nominare solo fornitori (pertanto esterni al tuo Studio) che siano in grado di fornire "sufficienti garanzie" sulla protezione delle informazioni dei clienti, la tutela dei loro diritti e l'assolvimento dei requisiti richiesti dal Regolamento.
I fornitori (indicati con il termine "processors" nel Regolamento) devono agire solo in base alle istruzioni documentate. Hanno comunque alcuni obblighi e responsabilità diretti ai sensi del Regolamento. Violazioni ai requisiti del regolamento possono determinare l'erogazione di sanzioni, misure correttive, risarcimento danni in procedimenti giudiziari.
In futuro saranno disponibili codici di condotta o schemi di certificazione emanati dalle Autorità di controllo a cui aderire al fine di ricondurre le modalità operative e le clausole contrattuali entro schemi approvativi ed operativi certi.

Rischi informativi

- **Il tuo Studio gestisce i rischi delle informazioni in modo strutturato così che sia valutato l'impatto sul business dei rischi relativi ai dati personali e siano gestiti in modo efficace?**

Le modalità di gestione del rischio informativo dovrebbero essere chiare e riportate in un documento che descrive le modalità di conduzione delle analisi dei rischi e la loro valutazione.
Laddove sono stati individuati rischi informativi, la relazione di analisi dei rischi deve indicare opportuni piani di azione per mitigare eventuali rischi non tollerati o risolti.

Protezione dei dati in base al design

- **Il tuo Studio ha implementato adeguate misure tecniche e organizzative per integrare la protezione dei dati nelle sue attività di elaborazione?**

i sensi del Regolamento, il tuo Studio ha l'obbligo generale di attuare misure tecniche e organizzative adeguate a dimostrare di aver preso in considerazione e integrato la protezione dei

dati nelle proprie attività di elaborazione. Questa protezione dei dati è intesa come protezione per impostazione predefinita, valutata in sede di progettazione del trattamento e ritenuta idonea a garantire i livelli di sicurezza delle informazioni richiesti dalla criticità delle stesse.
È inoltre necessario adottare politiche interne e attuare misure che consentano di rispettare i principi di protezione dei dati, tra cui la minimizzazione dei dati, la pseudonimizzazione e le misure di trasparenza.

Valutazioni di impatto sulla protezione dei dati (DPIA)

- **Il tuo Studio è in grado di stabilire la necessità di valutazioni di impatto sulla protezione dei dati (DPIA) ed ha processi attivi per effettuarle?**

Le valutazioni di impatto sulla protezione dei dati (DPIA) aiutano a identificare il modo più efficace per rispettare gli obblighi di protezione dei dati e soddisfare le aspettative della privacy degli interessati.
Una DPIA efficace consentirà di identificare e risolvere i problemi in una fase iniziale, riducendo i costi associati e i danni alla reputazione che potrebbero altrimenti verificarsi.
È necessario eseguire una valutazione d'impatto (DPIA) prima di iniziare qualsiasi tipo di elaborazione che "potrebbe comportare un rischio elevato". Ciò significa che, sebbene non sia stato ancora valutato l'effettivo livello di rischio, è necessario selezionare fattori che indichino un potenziale impatto diffuso o grave sulle informazioni personali degli interessati.
In particolare, il Regolamento richiede una DPIA per i trattamenti che:

- utilizzano una profilazione sistematica e approfondita con effetti significativi;
- elaborano una categoria speciale o dati di reato su vasta scala; o
- monitorano sistematicamente i luoghi accessibili al pubblico su larga scala (ad es. telecamere di controllo nelle stazioni ferroviarie).

Una valutazione di impatto (DPIA) è richiesta anche se si:

- utilizzano nuove tecnologie;
- utilizzano i dati di profilazione o delle categorie speciali per decidere l'accesso ai servizi;
- profilano gli individui su larga scala;
- elaborano dati biometrici o dati genetici;
- abbinano i dati o combinano set di dati provenienti da fonti diverse;
- raccolgono dati personali da una fonte diversa dall'individuo senza fornire avvisi sulla privacy;
- tracciano la posizione o il comportamento degli individui;
- elaborano dati che potrebbero mettere in pericolo la salute fisica o la sicurezza dell'interessato in caso di violazione della sicurezza.

Anche in assenza di indicazioni specifiche di probabile rischio elevato, è opportuno effettuare una DPIA per qualsiasi nuovo importante progetto che prevede l'uso di dati personali.
La DPIA dovrebbe contenere le seguenti informazioni:

- una descrizione della natura, della portata, del contesto e delle finalità del trattamento e, ove applicabile, degli interessi legittimi perseguiti dalla vostra azienda;
- una valutazione della necessità e proporzionalità del trattamento in relazione allo scopo della raccolta di dati personali;
- una valutazione obiettiva dei rischi per gli individui, considerando sia la probabilità di accadimento che l'impatto del possibile danno; e
- quali contromisure sono stati identificate per affrontare questi rischi e con quali risultati (eliminazione, riduzione, accettazione).

Se il "rischio residuo" dopo che sono state prese tutte le misure di attenuazione rimane elevato è richiesto di consultare l'Autorità Garante prima di procedere al trattamento dei dati personali.

Responsabili della protezione dei dati (DPO)

- **Il tuo Studio ha valutato la necessità e, nel caso, nominato un responsabile della protezione dei dati (DPO)?**

La nomina di un responsabile della protezione dei dati (DPO) è richiesta solo se:

- il titolare del trattamento è un'autorità pubblica;
- viene effettuato un monitoraggio regolare e sistematico su larga scala delle persone (es. monitoraggio del comportamento online); o
- vengono effettuate elaborazioni su larga scala di categorie speciali di dati o dati relativi a condanne penali e reati (si fa riferimento ad una soglia minima di 200-250 soggetti interessati, ma la valutazione di "larga scala" è responsabilità del Titolare).

Potrebbe risultare utile designare un DPO su base volontaria anche quando il Regolamento non richiede di farlo.
Il responsabile della protezione dei dati deve lavorare in modo indipendente, riferire al massimo livello di gestione e disporre di risorse adeguate per verificare che l'organizzazione soddisfi ai propri obblighi di conformità al Regolamento.
I compiti minimi del DPO sono:

- informare e consigliare l'organizzazione e i suoi dipendenti circa i loro obblighi di conformità con il Regolamento e altre leggi sulla protezione dei dati;
- monitorare la conformità con il Regolamen-

to e altre leggi sulla protezione dei dati, compresa la gestione delle attività interne di protezione dei dati, la sensibilizzazione e la formazione del personale e la conduzione di audit interni;
- fornire consulenza e monitorare le valutazioni d'impatto sulla protezione dei dati;
- rappresentare il punto di contatto con l'Autorità Garante; e
- rappresentare il punto di contatto per le persone i cui dati vengono elaborati (dipendenti, clienti, ecc.).

Responsabilità della gestione

- **Il responsabile dello Studio dimostra e documenta il suo supporto all'attuazione della protezione dei dati e promuove una cultura positiva di conformità alla normativa?**

I responsabili delle decisioni in azienda e le persone chiave dovrebbero:
essere a conoscenza dei requisiti del Regolamento Generale sulla Protezione dei Dati personali (RGPD);
- dare l'esempio, dimostrando la responsabilità per il rispetto del RGPD e promuovendo in azienda una cultura positiva per la protezione dei dati;
- assumere un ruolo guida nel valutare eventuali impatti sulla propria attività e incoraggiare un approccio basato sulla privacy in base alla progettazione;
- aiutare a stimolare la consapevolezza di tutto il personale sull'importanza di esercitare buone pratiche di protezione dei dati.

6.6.4 Sicurezza dei dati, trasferimenti internazionali e violazioni

Politica di sicurezza

- **Il tuo Studio ha una politica di sicurezza delle informazioni che attua appropriate misure di sicurezza?**

È necessario stabilire e attuare una politica di sicurezza delle informazioni che ne illustri l'approccio aziendale, le misure tecniche e organizzative applicate e i ruoli e le responsabilità assegnate al personale in relazione al mantenimento delle informazioni.
È necessario garantire una sicurezza appropriata ai dati personali raccolti, sulla base di valutazioni del rischio e scelta delle misure di sicurezza idonee alle esigenze.

Le scelte di sicurezza e protezione dei sistemi IT richiedono tempo, risorse e (potenzialmente) esperienza specialistica per adottare le misure tecniche e organizzative appropriate ed adeguate alle esigenze del tuo Studio.

Notifica di violazione

- **Il tuo Studio ha processi efficaci per identificare, segnalare, gestire e risolvere eventuali violazioni dei dati personali?**

Il Regolamento introduce l'obbligo, per tutte le organizzazioni, di segnalare all'Autorità Garante senza indebito ritardo, ma non più tardi di 72 ore, alcuni tipi di violazioni della sicurezza dei dati personali che potrebbero portare alla distruzione, perdita, alterazione, divulgazione non autorizzata o illegale delle informazioni personali.
Inoltre, se la violazione può comportare un rischio elevato per i diritti e le libertà delle persone fisiche, è necessario informare gli interessati direttamente e senza indebito ritardo.
In tutti i casi è necessario conservare un registro delle violazioni dei dati personali, indipendentemente dal fatto che siano soggette all'obbligo di notifica all'Autorità Garante.
È necessario assicurarsi di disporre di una procedura di rilevamento delle violazioni, indagini e reporting interno, che faciliterà il processo decisionale in merito alla necessità di informare l'Autorità Garante o le persone interessate.
Alla luce dei tempi stretti per la segnalazione di una violazione, è importante disporre di solide procedure.
È importante ricordare che è necessario segnalare una violazione senza indebito ritardo e comunque entro 72 ore da quando se ne viene a conoscenza.

Trasferimenti internazionali

- **Il tuo Studio garantisce un livello adeguato di protezione per i dati personali laborati da terzi a vostro nome e verifica la legittimità di eventuali trasferimenti al di fuori dello Spazio economico europeo?**

Il Regolamento impone restrizioni al trasferimento di dati personali al di fuori dell'Unione Europea, a paesi terzi o organizzazioni internazionali. Queste restrizioni permettono il trasferimento di dati personali al di fuori dell'UE a condizione che il paese destinatario rispetti i requisiti descritti nel regolamento e sia nell'elenco di quelli autorizzati.

Note

1 Il termine in italiano è Regolamento Generale sulla Protezione dei Dati (RGDP), ma in questa sede si preferisce fare riferimento alla sigla in lingua inglese in quanto di uso comune.

2 Si ricorda qui a titolo di esempio che la Direttiva 2002/58/CE del Parlamento europeo e del Consiglio (relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche) era in corso di aggiornamento attraverso il così detto Regolamento ePrivacy che però non è arrivato ad approvazione finale in accordo fra Commissione Europea e Parlamento Europeo e sarà soggetto ad un nuovo iter complessivo di scrittura ed approvazione.

3 il D.Lgs. 101:2018 che ha adeguato la normativa nazionale – il D.Lgs. 196:2003 – alla normativa europea ha avuto una lunga gestazione ed è stato approvato il 10 agosto 2018, quindi dopo l'entrata in efficacia del GDPR.

4 Traduzione del concetto espresso con il termine inglese "Accountability".

5 Esula dagli obiettivi della linea guida la trattazione esaustiva di tutti gli adempimenti.

6 Lo svolgimento di attività di consulenza in ambito di protezione dei dati personali necessità di una conoscenza molto approfondita del quadro normativo e di best practice ad esso connesse.

7 Sono note anche con il termine inglese Data Breach.

8 Il termine interessati è un'eredità della normativa del '95 ed è una traduzione del termine inglese Data Subject utilizzato nativamente dalla normativa; il termine interessato sta quindi ad indicare il soggetto a cui si riferisce il dato personale da qui interessato (sottinteso, del dato personale).

9 Il GDPR ha formalizzato l'esistenza di tecniche intermedie rispetto all'anonimizzazione. La pseudonimizzazione è un'anonimizzazione che può essere reversibile, in determinate circostanze, e che può semplificare il trattamento dei dati personali in determinate situazioni andandoli, per così dire, a "desensibilizzare".

10 Si fa qui un inciso importante: la normativa si applica ai dati personali che, quindi, devono essere protetti "per legge". Sugli altri dati o informazioni gestite dagli ingegneri e dagli studi associati (dati di clienti aziende, progetti, ecc.) non si applica la normativa GDPR (potrebbero però applicarsene delle altre), ma non significa che questi dati non debbano essere protetti.

11 È qui opportuno fare una considerazione nell'ambito della professione: nelle realtà di studi professionali individuali o di studi associati è comune una commistione fra privato e lavorativo che solitamente è più netta in ambiti più grandi. Nelle realtà piccole è comune -ad esempio- che il cellulare privato è anche quello aziendale così come la email, è altresì possibile che l'indirizzo di casa e di ufficio coincidano. In questi casi risulta più difficile la distinzione fra dati personali e giuridici (cioè del professionista in quanto ditta individuale). In questi casi l'approccio prudenziale da utilizzare è quello del dato più critico: se si hanno sia clienti privati che professionisti, nello stesso archivio coesisteranno dati personali (anagrafica di persone fisiche) e dati non personali (anagrafica di aziende). Questo archivio va considerato come se contenesse tutti dati personali che ricadono quindi nell'ambito di applicazione della normativa privacy.

12 In questa sezione si preferisce fare riferimento all'organizzazione in termini generali e non all'ingegnere professionista o allo studio associato in quanto questo concetto è generale e valido non solo in questi specifici contesti.

13 Questa figura non è differente da quella definita nella precedente normativa (Direttiva 46/95/CE e, in Italia, con il Decreto Legislativo 196:2003 prima delle ultime modifiche apportate dal Dlgs 101:2018).

14 È anche noto come Garante Privacy.

15 Questa Autorità normalmente non ha a che fare con l'ingegnere professionista o gli studi associati in quanto è l'autorità a cui possono fare riferimento i cittadini europei per quanto attiene i loro rapporti con le istituzioni europee. Lo si è aggiunto nei ruoli per completezza e per chiarirne il ruolo che non è quello di Garante "superiore" ai Garanti nazionali, ruolo invece assegnato al Comitato europeo per la protezione dei dati.

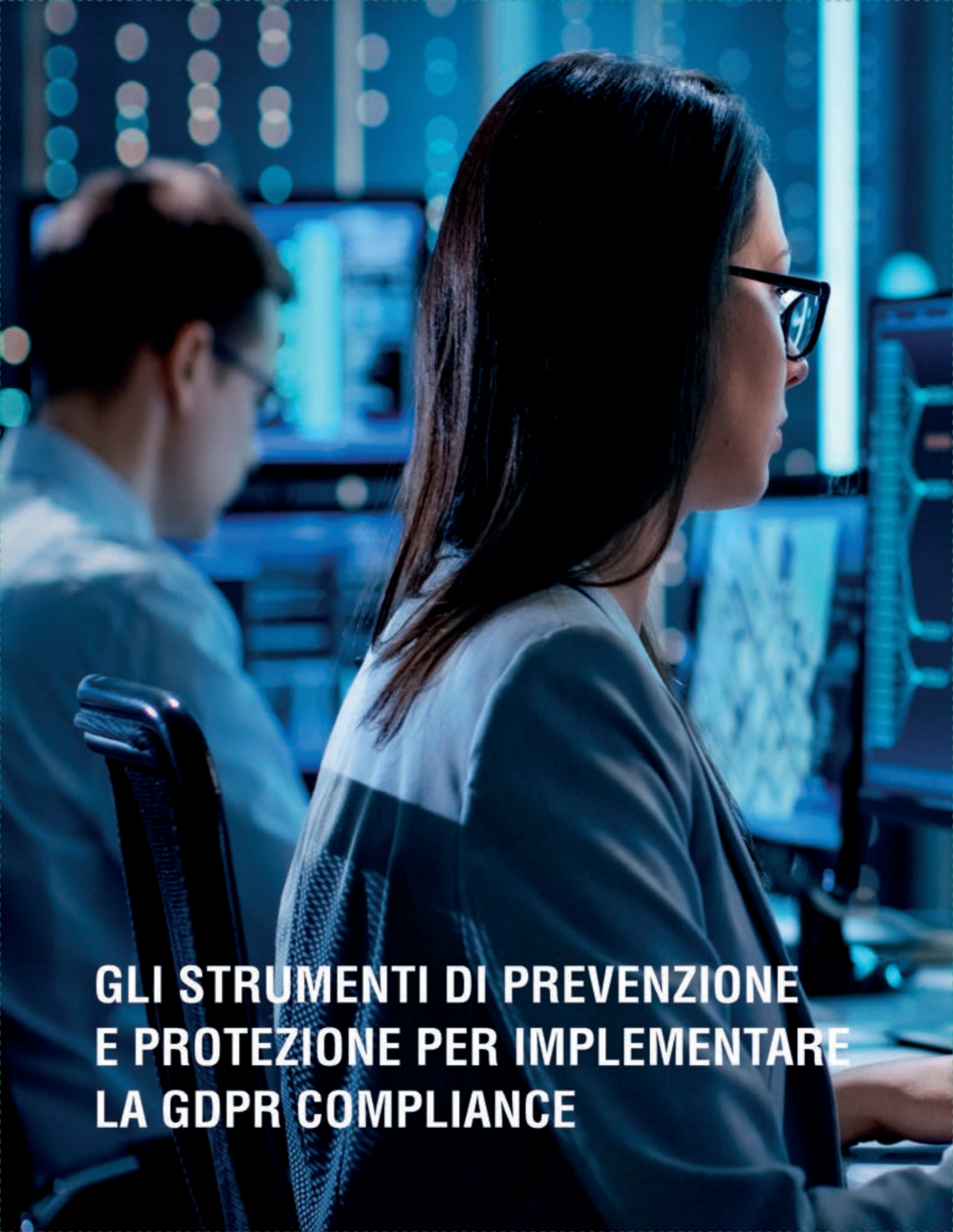
16 Il Garante della Protezione dei Dati personali.

17 In questo caso il professionista deve essere nominato dal suo cliente come Responsabile del Trattamento, detta nomina può essere parte del contratto stesso intercorso fra le parti o come documento separato che va ad integrare il contratto stesso (PDA - Privacy Data Agreement).

18 Questo può accedere qualora due Ingegneri professionisti (ma anche un Ingegnere ed altro professionista quale Architetto, Commercialista, Avvocato, Geometra o altro) condividono lo stesso studio mantenendo comunque la loro separazione professionale. Nella condivisione dello studio condividono anche alcuni sistemi, archivi o altro con informazioni dei clienti.

19 A titolo di semplificazione per "Finalità" del trattamento si intende la motivazione o lo scopo per cui sono stati richiesti, raccolti, sono archiviati e sono utilizzati questi dati.

20 Questa semplificazione è stata probabilmente inserita per venire incontro a contesti come i professionisti o le micro o piccole imprese per semplificare gli adempimenti. Persistendo comunque l'obbligo in alcuni casi risulta non del tutto chiaro come si possa valutare l'esistenza di trattamenti che ne richiederebbero l'obbligo senza averne individuato il trattamento stesso.
21 cfr. Par. 3.4.
22 Esistono diversi servizi web gratuiti e a pagamento che permetto di predisporre moduli web. Nell'utilizzo di questo genere di servizi risulta particolarmente importante verificare le condizioni di utilizzo del servizio.
23 A titolo di esempio il Garante della Protezione dei Dati Personali ha fornito pareri specifici sui tempi di conservazione dei dati per finalità di marketing dipendenti dal ciclo di vita del bene.
24 Esplicito non è da intendersi sinonimo di scritto.
25 Le misure qui riportate sono delle indicazioni di possibili misure di sicurezza semplici che possono essere implementate all'interno di uno studio professionale al fine di incrementare la sicurezza della riservatezza, dell'integrità e della disponibilità dei dati personali e delle informazioni gestiste dallo studio (ad esempio progetti). Sono solo alcuni esempi e non hanno la pretesa di essere esaustivi. Possono essere considerate come una sorta di "misure minime" consigliate.
26 È nota in letteratura anche come Privacy impact Assessment – PIA.
27 https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9058979
28 È importante precisare che tali misure di sicurezza indicate all'interno dell'Art. 25 del GDPR sono probabilmente da intendersi a titolo di esempio in quanto non sono le uniche che concorrono alla protezione dei dati personali.
29 Il titolare viene a conoscenza della violazione nel momento in cui si è accorto che si è verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali.
30 Per completezza si ricorda che la struttura del D.Lgs. 196/03 al momento della sua approvazione era anomala in quanto includeva un disciplinare tecnico come allegato di una legge. L'intento del legislatore italiano era quello di fornire misure di sicurezza che avrebbero dovuto essere aggiornate nel tempo, cosa che non è mai avvenuta in quanto il disciplinare restò fermo alla prima emissione. Va inoltre ricordato che la precedente normativa vigente in Italia indicava comunque la necessità di misure idonee e non solo di quelle minime.
31 Aspetto importante è che quando si parla di rischio il punto di vista è quello dell'interessato e non dell'organizzazione, cioè le misure di sicurezza devono essere pensate in funzione del cittadino (o cliente) che è l'anello debole della catena e non dell'organizzazione. Ad es. un rischio di perdita di immagine dell'organizzazione a seguito di un Violazione dei dati (Data breach) non è il rischio a cui fa riferimento il dovere normato, mentre lo è quello del cittadino qualora venissero resi pubblici dati personali non adeguatamente protetti.
32 Alla data di redazione delle presenti linee guida non sono ancora disponibili codici di condotta, mentre sono in corso di valutazione degli schemi di certificazione sia a livello nazionale che europei. In particolare, in Italia è stato già accreditato da Accredia lo schema di certificazione ISDP@10003 per determinare la conformità al GDPR delle organizzazioni (https://www.accredia.it/servizio-accreditato/protezione-dei-dati-personali/).
33 Il DPS includeva normalmente oltre al Registro delle Attività di Trattamento anche altri aspetti quali l'analisi dei rischi, le misure di sicurezza adottate, ecc.
34 In questa sede si preferisce utilizzare i termini in lingua inglese e non quelli della traduzione in italiano che sono "Protezione dei dati fin dalla progettazione" e "Protezione per impostazione predefinita".
35 Va precisato che anche se non presente a livello di normativa il principio di privacy by design era presente a livello di interpretazione delle Autorità garanti della protezione dei dati in quanto da queste adottato nella 32a Conferenza Internazionale delle Autorità di Protezione dei Dati tenutasi a Gerusalemme a ottobre 2010.
36 Il GDPR e il regime sanzionatorio che introduce sono generali a tutte le organizzazioni, quindi è applicato sia all'ingegnere professionista che al colosso del web. Il regime sanzionatorio precedente prevedeva importi ridotti che potevano non impensierire le aziende di grandi dimensioni, mentre quello attuale -proporzionale- rende potenzialmente pericolose sotto il profilo economico le politiche di sottovalutazione in merito al trattamento dei dati personali.
37 https://www.garanteprivacy.it/home/faq/informativa-e-consenso-per-uso-cookie
38 https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/803679339
39 https://www.garanteprivacy.it/home/faq/informativa-e-consenso-per-uso-cookie
40 https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8036793



GLI STRUMENTI DI PREVENZIONE E PROTEZIONE PER IMPLEMENTARE LA GDPR COMPLIANCE

Quaderno

a cura di
Ing. Paola Rocco

Le soluzioni di raccolta e monitoraggio degli eventi hanno come obiettivo la raccolta centralizzata degli eventi di sicurezza generati da applicazioni e sistemi, al fine di garantire la conformità alle normative e quindi ridurre i tempi necessari alla risoluzione degli allarmi e dei possibili incidenti di sicurezza. Sono quindi uno strumento fondamentale per ottemperare a quelle che sono le indicazioni del GDPR e in modo più ampio per effettuare la protezione dei dati.
Molto spesso tali strumenti nelle architetture più evolute e complete sono utilizzati anche come raccoglitori degli eventi di sicurezza o "log collector" veri e propri aggiungendo alle funzionalità di sicurezza anche requisiti quali immodificabilità delle informazioni memorizzate. Tali soluzioni sono indicate con l'acronimo SIEM, cioè Security Information and Event Management. Un SIEM si occupa quindi della raccolta, aggregazione, normalizzazione e storicizzazione di eventi rilevanti; la raccolta di dati contestualizzati; l'analisi, incluse la correlazione e prioritizzazione degli eventi; la presentazione, incluse la reportistica e la visualizzazione dei dati. Per questi motivi è lo strumento fondamentale su cui basare l'attività di un Security Operation Center (SOC) di un'azienda.
La stessa piattaforma poi deve essere progettata in conformità alle norme nazionali, internazionali e ai framework di sicurezza richiesti dalle esigenze di business tra cui anche lo stesso (UE) 2016/679 o GDPR.
I SIEM hanno fatto la loro comparsa sul mercato diversi anni fa a partire dal 1997. Inizialmente, il loro obiettivo era solo quello di ridurre i falsi positivi generati dalle infrastrutture di sicurezza (ad esempio NIDS Network Intrusion Detection System) che quotidianamente generavano un quantitativo enorme di alert o eventi rendendo impossibile la loro gestione. La seconda generazione del SIEM ha anche permesso di migliorare la reportistica e i cruscotti di visualizzazione delle informazioni, oltre a fornire la possibilità di interrogare per la prima volta i dati storici memorizzati.
La terza generazione di SIEM ha introdotto una rivoluzione radicale tramite l'introduzione , di algoritmi di machine learning, integrando Threat Intelligence e analisi comportamentale dell'utente e delle entità (UEBA User and Entity Behavior Analytics).
Il SIEM quindi, è la soluzione tecnologica che analizza le informazioni raccolte per evidenziare eventi o comportamenti di interesse consentendo, ad esempio, di rilevare un accesso amministrativo al di fuori del consueto orario di lavoro, fornendo anche la possibilità di fare analisi di dettaglio, ad esempio analizzando le informazioni sull'apparato che lo ha generato o sull'evento stesso.
Le correlazioni generate dalle piattaforme SIEM

sono degli eventi aggregati che consentono di relazionare dati significativi provenienti da molteplici fonti, per poi individuare deviazioni, anomalie rispetto alla norma, e far scattare allarmi ed analisi specifiche dell'evento che potrebbe diventare un possibile incidente.
Con il termine Threat Intelligence e analisi comportamentale UEBA (user behavior entity analytics) si intendono le componenti dei SIEM che analizzano il comportamento degli utenti come mezzo per aiutare a rilevare e bloccare le minacce interne. Gli strumenti UEBA sfruttano la tecnologia di apprendimento automatico per analizzare un gruppo di utenti, identificando i valori anomali che potrebbero essere potenziali minacce interne.
Vediamo ora le funzionalità che caratterizzano

le piattaforme per la raccolta e il monitoraggio degli eventi (SIEM). Tali funzionalità sono:

- La raccolta di log e dati contestualizzati attraverso la definizioni di processi informatici basati anche su agenti specifici per ogni prodotto software;
- La rappresentazione dei log raccolti in un formato universale che ne permetta la corretta lavorazione all'interno del SIEM. Gli eventi, inoltre, per poter essere facilmente gestiti sono inoltre classificati in specifiche tipologie come "modifiche di configurazione", "accesso ai file" o "attacco buffer overflow" e così via;
- La correlazione tra eventi diversi generati da diverse fonti dati. La correlazione può avvenire in tempo reale, e può utilizzare anche tabelle statiche o liste che possono identificare ulteriormente l'evento stesso (ad esempio si può utilizzare una lista di indirizzi IP o di nomi macchina per identificare le risorse interne da proteggere).
- La generazione di notifiche o avvisi che sono inviati a operatori del SOC (Security Operation Centre) o manager. I meccanismi di avviso più diffusi includono e-mail, SMS o semplici messaggi SNMP (Simple Network Management Protocol).
- Le funzionalità che aiutano a mettere in evidenza gli eventi importanti rispetto a quelli meno critici, per classificarli e prioritizzarli correlando ad esempio gli eventi di sicurezza con le informazioni sulla vulnerabilità, l'importanza dell'asset;

- La possibilità di creare dashboard di monitoraggio della sicurezza e sezioni specifiche utilizzate dal personale operativo. Tali visualizzazioni mostrano agli analisti di sicurezza le informazioni raccolte e i risultati delle correlazione in tempo reale.
- La reportistica che aiuta ad evidenziare lo stato di sicurezza della rete, l'andamento di possibili attacchi o il traffico anomalo. Tale sezione può essere customizzata a piacere per generare delle Console dedicate per gli operatori del SOC, o il Management che deve prendere delle decisioni.
- La funzionalità di gestione degli incidenti, automatica o semiautomatica, quali l'apertura di casi e l'esecuzione di attività di indagine. La maggior parte degli strumenti infatti supporta l'integrazione nei principali sistemi di Ticketing esistenti.

Supponiamo di voler generare un allarme ogni qualvolta un utente faccia login su un server utilizzando credenziali amministrative locali e supponiamo che all'interno dell'organizzazione siano presenti sia dei server Windows e server Linux. Normalmente dovremmo abilitare i log all'interno dei diversi sistemi, raccoglierli e correlarli, mentre in un SIEM, utilizzando la logica interna, e nel caso di agent standard è possibile raccogliere i log normalizzarli e definire regole avanzate basate su diverse variabili quali ad esempio correlazioni e allarmi specifici.
Il correlation engine del SIEM permette di definire delle regole comuni che consentono di corre-

lare i diversi eventi scaturiti in un singolo evento di sicurezza, che possa generare poi un allarme e quindi un nuovo evento sul sistema. Generalmente i SIEM hanno una console, che può essere web-based o nel modello client-server, che serve per configurare, gestire e utilizzare il SIEM stesso da parte di diverse tipologie di utenti.

Le diverse tipologie di fonti dati da integrare devono essere identificate mediante i risultati dell'ultimo Risk Assessment per determinare le minacce, le vulnerabilità e identificare gli asset coinvolti, i sistemi critici da proteggere, i controlli applicabili. La piattaforma stessa, poi può essere utilizzata anche per fornire informazioni sull'attuale livello di sicurezza delle configurazioni dei sistemi monitorati e dei software installati, sempre se la configurazione sia completa e raccolga i dati di tutti gli asset esistenti da proteggere.
Inoltre fornisce un quadro sugli incidenti aperti, i sistemi sotto attacco, fornisce quindi le informazioni sulle procedure di reazione ed escalation messe in atto allo scopo di circoscrivere l'attacco.
Si comprende quindi come questi strumenti automatici opportunamente configurati per evitare falsi positivi, gestiti ed integrati nei processi aziendali, possano essere un valido strumento per identificare, analizzare gli eventi di sicurezza e garantire la conformità a norme e regolamenti.
La centralizzazione delle informazioni permette inoltre di favorire la conformità con il requisito espresso dall'articolo 32 del GDPR (Security of processing), con particolare riguardo all'adeguatezza delle "misure tecniche e organizzative".

a cura di
Ing. Natale Castelliti

LA DIRETTIVA EPRIVACY E IL RAPPORTO CON IL GDPR

1. La direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche

La direttiva ePrivacy nasce nel 2002, viene modificata nel 2006 dalla direttiva 2006/24/CE e in seguito nel 2009 dalla direttiva 2009/236/CE. Si occupa di trattamento dei dati personali e della tutela della vita privata nel settore delle comunicazioni elettroniche.
Nel 2002 non sono ancora nati i social network (Facebook nasce il 2004) nè gli strumenti di comunicazione vocale e video via computer, come Skype. Allo stesso tempo si assiste al fiorire di diverse proposte di motori di ricerca (Yahoo!, Google sono rispettivamente del 1995 e 1997) oltre che ad uno sviluppo di mercato della telefonia basata su VoIP.
Da qui nasce la necessità di questa direttiva che nel considerando 6 recita "L'Internet ha sconvolto le tradizionali strutture del mercato fornendo un'infrastruttura mondiale comune per la fornitura di un´ampia serie di servizi di comunicazione elettronica. I servizi di comunicazione elettronica accessibili al pubblico attraverso l'Internet aprono nuove possibilità agli utenti ma rappresentano anche nuovi pericoli per i loro dati personali e la loro vita privata."
In quell'anno la gestione dei dati personali è affidata, nell'UE, alla direttiva 95/46/CE, della quale la Direttiva ePrivacy traduce i principi enunciati in norme specifiche per il settore delle comunicazioni elettroniche. La 95/46/CE, pur nella sua innovatività, è destinata ad affrontare il mondo delle comunicazioni in grande fermento con l'arrivo del nuovo secolo.
Al 1997 risale invece la direttiva 97/66/CE del 15 dicembre 1997 sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni, abrogata dalla stessa Direttiva ePrivacy.
Vediamo, qui di seguito, le principali novità introdotte dalla Direttiva ePrivacy, così come descritti dalla Newsletter del Garante per la Protezione dei Dati personali del 29 luglio dello stesso anno: "Maggiore privacy per telefonia ed Internet dal Parlamento europeo"

- Conferma europea delle scelte già operate dal legislatore italiano per l'invio di e-mail commerciali e pubblicitarie solo agli utenti che abbiano espresso il proprio consenso.
- Divieto di inviare messaggi di posta elettronica, a scopo di direct marketing, omettendo o camuffando l'identità del mittente o senza l'indicazione di un indirizzo valido, cui il destinatario possa inviare una richiesta di cessazione.
- Regolamentazione dell'uso di cookies, spyware e bug.
- Particolare tutela per i dati relativi alla lo-

calizzazione dei cellulari raccolti nel corso della fornitura di nuovi tipi di servizi erogati da reti cellulari e satellitari che consentono di individuare esattamente l'apparecchiatura terminale dell'utente.

- Iscrizione negli elenchi telefonici pubblici, cartacei o elettronici, solo con il consenso degli abbonati e secondo modalità da loro scelte. dovranno conformarsi alle nuove disposizioni europee entro il 31 ottobre 2003.

(...)

Nella direttiva si sollecita inoltre la progettazione di sistemi di fornitura di reti e servizi di comunicazione che limitino al minimo la quantità di dati personali necessari. Si prevede che i dati dei naviganti in Internet possano essere conservati dopo l'erogazione del servizio per il quale sono stati forniti, al pari di quelli delle chiamate telefoniche, ai fini della fatturazione e del pagamento per interconnessione.
Ogni ulteriore trattamento deve essere autorizzato dall' abbonato. Ad esempio, se il provider vuole commercializzare altri prodotti o fornire servizi a valore aggiunto (orientamento stradale, previsioni meteorologiche, informazioni tariffarie o turistiche) deve raccogliere uno specifico consenso del cliente.
Per quanto riguarda il settore della telefonia la direttiva conferma il principio generale, già affermato nella 97/66/CE, che i dati sul traffico dell'utente devono essere cancellati o resi anonimi al termine della comunicazione. Permette comunque, entro precisi limiti e sulla base di determinate garanzie, la possibilità di introdurre delimitati tempi di conservazione laddove vi siano necessità di interventi proporzionali per finalità di accertamento e prevenzione di reati o motivi di sicurezza nazionale".
La Direttiva ePrivacy viene recepita in Italia con il ben noto decreto legislativo 196 del 2003.

2. La direttiva 2006/24/CE riguardante la conservazione di dati generati o trattati nell'ambito

della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE

Il panorama politico sociale di inizio secolo è fortemente caratterizzato da insicurezza e senso di pericolo per il propagarsi degli attentati terroristici. Dopo l'11 settembre 2001, si registrano in Europa l'attentato di Madrid dell'11 marzo 2004 e quello di Londra del 7 luglio 2005. In vista di una maggiore attenzione alla prevenzione degli attentati, la politica comunitaria si indirizza verso decisioni finalizzate ad incrementare il tempo di conservazione dei dati delle comunicazioni. Questo fa si che l'intelligence possa ampliare la base di dati attraverso la quale sia in grado sia di valutare preventivamente il movimento di traffici sospetti sia di reagire efficacemente ad aggressioni organizzate e premeditate. Nasce in questo clima la direttiva 2006/24/CE che si propone di *"armonizzare le disposizioni degli Stati membri relative agli obblighi, per i fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione, relativi alla conservazione di determinati dati da essi generati o trattati, allo scopo di garantirne la disponibilità a fini di indagine, accertamento e perseguimento di reati gravi, quali definiti da ciascuno Stato membro nella propria legislazione nazionale" – Art.1 par.1*

La Direttiva ePrivacy non dava indicazioni precise sui tempi di conservazione dei dati, puntando fondamentalmente alla loro sicurezza e riservatezza, lasciando un generico margine di eccezione a salvaguardia della sicurezza pubblica ovvero prevenzione e perseguimento di reati (art.15).

Al contrario la nuova direttiva obbliga i fornitori di servizi a conservare i dati delle comunicazioni e ne stabilisce le modalità.

In particolare, l'art.1 par. 2 fissa un punto fermo: *La presente direttiva si applica ai dati relativi al traffico e ai dati relativi all'ubicazione delle per-*

sone sia fisiche che giuridiche, e ai dati connessi necessari per identificare l'abbonato o l'utente registrato. ***Non si applica al contenuto*** *delle comunicazioni elettroniche, ivi incluse le informazioni consultate utilizzando una rete di comunicazioni elettroniche.*

Relativamente ai dati di traffico, è l'articolo 5 a dettare cosa si intende (prendendo in considerazione di caso in caso la telefonia di rete fissa, la telefonia mobile, Internet, posta elettronica su Internet e telefonia via Internet):

a) i dati necessari per rintracciare e identificare la fonte di una comunicazione

b) i dati necessari per rintracciare e identificare la destinazione di una comunicazione

c) i dati necessari per determinare la data, l'ora e la durata di una comunicazione

d) i dati necessari per determinare il tipo di comunicazione:

e) i dati necessari per determinare le attrezzature di comunicazione degli utenti o quello che si presume essere le loro attrezzature

f) i dati necessari per determinare l'ubicazione delle apparecchiature di comunicazione mobile

... e ribadisce a conclusione: A norma della presente direttiva, non può essere conservato alcun dato relativo al **contenuto della comunicazione.**

Relativamente ai tempi di conservazione, l'articolo 6 recita "Gli Stati membri provvedono affinché le categorie di dati di cui all'articolo 5 siano conservate per periodi non inferiori a sei mesi e non superiori a due anni dalla data della comunicazione."

Nel corso degli anni successivi alla sua emanazione, la direttiva 2006/24/CE viene recepita dalle legislazioni nazionali; ben presto però si manifestano diverse iniziative aventi ad oggetto la verifica della legittimità delle misure nazionali inerenti la conservazione dei dati relativi alle comunicazioni elettroniche per tempi così lunghi. Queste iniziative culminano nella sentenza della Corte di Giustizia dell'8 aprile 2014, che recita definitivamente "La direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE, **è invalida**."

La causa di tale decisione è da collegare alla violazione del principio di proporzionalità in quanto, secondo la Corte, la direttiva:

1) ha previsto le misure di conservazione dei dati come applicabili in via indifferenziata e generalizzata "all'insieme degli individui, dei mezzi di comunicazione elettronica e dei dati relativi al traffico, senza che venga operata alcuna differenziazione, limitazione o eccezione in ragione dell'obiettivo della lotta contro i reati gravi";

2) ha omesso di prevedere alcun criterio oggettivo che limiti l'accesso a tali dati per sole esigenze di accertamento di reati "sufficientemente gravi da giustificare una simile ingerenza", ben oltre - dunque - il generico rinvio ai reati gravi definiti da ciascuno Stato membro;

3) ha omesso di sancire i presupposti sostanziali

e procedurali ai quali subordinare l'accesso, da parte delle competenti autorità nazionali, ai dati in esame, in particolare non richiedendo in ogni caso il previo controllo dell'autorità giudiziaria o di un'autorità amministrativa indipendente;
4) ha omesso di prevedere criteri necessari a differenziare la durata della conservazione dei dati, limitandosi a stabilirne i soli termini minimi (6 mesi) e massimi (24);
5) ha omesso di imporre che i dati così acquisiti siano conservati nel (solo) territorio della Ue.

3. La direttiva 2009/136/CE del 25 novembre 2009 recante modifica (...) della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (...)

La direttiva 2009/136/CE introduce aggiornamenti in diversi provvedimenti precedenti tra cui la stessa direttiva ePrivacy. Le modifiche apportate al riguardano in particolare:

- nuovi obblighi in tema di sicurezza dei dati personali;
- gestione dei diritti dei contraenti/utenti in relazione all'uso dei dati personali;
- rafforzamento del processo di attuazione e del suo controllo.

Sicurezza dei dati

La sicurezza del trattamento, così come esposta nell'articolo 4, viene intensificata e rafforzata con criteri che anticipano il concetto di data breach del RGPD.
La versione ePrivacy del 2002 si limita a due paragrafi nei quali da una parte si parla di misure adeguate e limitate dai costi di realizzazione, dall'altra si paventa il rischio di violazione di sicurezza davanti al quale il fornitore di un servizio ha l'obbligo di informare gli abbonati indicando, qualora il rischio sia al di fuori del campo di applicazione delle misure che devono essere prese dal fornitore di servizio, tutti i possibili rimedi, compresi i relativi costi presumibili.
Con la 2009/136/CE vengono aggiunti altri tre paragrafi con i seguenti obiettivi:

- estendere il concetto di dato personale non al solo abbonato ma ad altra persona interessata,
- prendere in considerazione il caso di violazione di dati personali. In particolare:
  - il fornitore di servizi di comunicazione elettronica ha l'obbligo di comunicare senza indebiti ritardi detta violazione all'autorità nazionale competente;
  - se la violazione rischia di pregiudicare i dati personali o la vita privata di un abbonato o di altra persona, il fornitore ha l'obbligo di comunicare l'avvenuta violazione anche all'abbonato o ad al tra persona interessata;
  - il fornitore si esime dall'obbligo della notifica a un abbonato o a una persona interessata se dimostra in modo con vincente all'autorità competente di aver utilizzato le opportune misure

tecnologiche di protezione, come per esempio la crittografia;
- La comunicazione all'abbonato o ad altra persona deve contenere almeno una descrizione della natura della violazione di dati personali e i punti di contatto presso cui si possono ottenere maggiori informazioni ed elenca le misure raccomandate per attenuare i possibili effetti pregiudizievoli della violazione di dati personali;
- La comunicazione all'autorità nazionale competente descrive, inoltre, le conseguenze della violazione di dati personali e le misure proposte o adottate dal fornitore per porvi rimedio;
- I fornitori hanno l'obbligo di mantenere un inventario delle violazioni dei dati personali, ivi incluse le circostanze in cui si sono verificate, le loro conseguenze e i provvedimenti adottati per porvi rimedio. Questo sia dedicato esclusivamente alle informazioni necessarie a tal fine;
- Viene coinvolta la Commissione europea per adottare misure tecniche finalizzate all'attuazione delle procedure applicabili nel presente articolo, dopo aver consultato l'ENISA (l'Agenzia europea per la sicurezza delle reti e dell'informazione), il WP29 (il gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali, istituito dall'articolo 29 della direttiva 95/46/CE, attuale EDPB – European Data Protection Board) e il Garante europeo della protezione dei dati.

Gestione dei diritti dei contraenti/utenti

Da questo punto di vista la normativa espressa dalla direttiva ePrivacy era già a livelli avanzati. In pratica la 2009/136/CE:

- conferma l'adozione dell'approccio Opt-In. Questo consiste nel considerare consentite le chiamate e comunicazioni senza operatore, telefax e posta elettronica, solamente se preventivamente autorizzate;
- conferma la possibilità di esercitare il diritto di opposizione in caso di ripensamento;
- sottolinea la possibilità che l'esercizio di detti diritti venga esercitato in modo facile e gratuito;
- ribadisce il divieto della prassi di camuffare il mittente nelle comunicazioni di posta elettronica finalizzati alla commercializzazione;
- sottolinea che gli stati membri debbano favorire il diritto di promuovere un'azione giudiziaria contro le possibili violazioni da parte di ogni persona fisica o giuridica che abbia subito effetti pregiudizievoli a seguito delle

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI ROMA

violazioni delle disposizioni nazionali adottate in recepimento del presente articolo.

Rafforzamento del processo di attuazione e del suo controllo

Con l'introduzione dell'articolo 15 bis, la direttiva 2009/136/CE:

- invita gli stati membri a definire le sanzioni, amministrative e penali, in presenza delle violazioni esaminate;
- invita gli stati membri ad adottare leggi di recepimento autorevoli, in grado cioè di mettersi in grado di ordinare la cessazione delle violazioni;
- richiede che le autorità locali dispongano delle risorse e delle competenze necessarie per l'esercizio delle proprie attività;
- sollecita la collaborazione con la Commissione nelle diverse fasi del processo, sempre in accordo con il WP29, l'ENISA, e il Garante europeo;
- sollecita l'adozione di misure che favoriscano il flusso di dati transfrontalieri.

4. Sviluppi conseguenti alla promulgazione del RGPD

Nel 2016 vede la luce, dopo diversi anni di lavoro, la versione definitiva del nuovo regolamento per la protezione dei dati personali, il Regolamento Generale sulla Protezione dei Dati (RGPD - ufficialmente regolamento n. 2016/679). Questo sostituisce la direttiva 95/46/CE ma, come regolamento dell'Unione, prevale sulla legislazione dei paesi membri, senza richiedere leggi di recepimento.

Il RGPD cita in diverse occasioni la direttiva ePrivacy:

- *il considerando 173 recita: È opportuno che il presente regolamento si applichi a tutti gli aspetti relativi alla tutela dei diritti e delle libertà fondamentali con riguardo al trattamento dei dati personali che non rientrino in obblighi specifici, aventi lo stesso obiettivo, di cui alla direttiva 2002/58/CE del Parlamento europeo e del Consiglio (18), compresi gli obblighi del titolare del trattamento e i diritti delle persone fisiche. Per chiarire il rapporto tra il presente regolamento e la direttiva 2002/58/CE, è opportuno modificare quest'ultima di conseguenza. Una volta adottato il presente regolamento, la direttiva 2002/58/CE dovrebbe essere riesaminata in particolare per assicurare la coerenza con il presente regolamento;*
- l'articolo 21 (Diritto di opposizione) recita

nel paragrafo 5: *Nel contesto dell'utilizzo di servizi della società dell'informazione e fatta salva la direttiva 2002/58/CE, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche;*

- l'articolo 95 (Rapporto con la direttiva 2002/58/CE) recita: *Il presente regolamento non impone obblighi supplementari alle persone fisiche o giuridiche in relazione al trattamento nel quadro della fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione nell'Unione, per quanto riguarda le materie per le quali sono soggette a obblighi specifici aventi lo stesso obiettivo fissati dalla direttiva 2002/58/CE.*

Come si vede dai precedenti punti, il regolamento non dà spiegazioni precise su come intendere il rapporto fra lo stesso RGPD e la direttiva ePrivacy, demandando tale compito a ulteriori spiegazioni e approfondimenti.

Nel frattempo, in recepimento di quanto suggerito dal considerando 173, il parlamento europeo si attiva per creare un aggiornamento della direttiva ePrivacy e anche in questo caso, novità, si orienta verso un regolamento piuttosto che ricreare una direttiva. A questo proposito il 10 gennaio 2017 viene presentata dalla Commissione una "Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche)".

La solerzia con cui questa bozza viene presentata, rispetto all'entrata in vigore del RGPD, e i punti della bozza citati qui sotto:

- Articolo 27 (Abrogazione) Paragrafo 1: La direttiva 2002/58/CE è abrogata a decorrere dal 25 maggio 2018,
- Articolo 29 (Entrata in vigore e applicazione) Paragrafo 2: Esso (ndr: il regolamento della bozza in questione) si applica a decorrere dal 25 maggio 2018,

fanno pensare ad una veloce riproposizione del nuovo regolamento, tale da poter entrare in vigore nella stessa data in cui il RGPD diventa pienamente operativo, il 25 maggio 2018.

Purtroppo, questo non avviene e, a distanza di più anni dall' ipotizzata entrata in vigore, non si ha traccia del nuovo regolamento né dell'uscita di nuove bozze. Si ipotizza che, a causa della struttura stessa del regolamento, che per sua natura non ammette adeguamenti locali, e della

necessità di un corretto equilibrio nel bilanciare opportunamente i diritti degli interessati con gli interessi di importanti player del mercato ivi inclusi gli OTT, il cammino di questo regolamento stia subendo un profondo rallentamento e probabilmente anche un profondo cambiamento rispetto alla stessa proposta del gennaio 2017.
E' probabilmente a causa di questo ritardo, del disappunto che ne consegue, della poca chiarezza che hanno gli operatori del campo della comunicazione elettronica in seguito all'entrata in vigore del RGPD, che l'EDPB pubblica un documento di approfondimento sull'interpretazione del rapporto che intercorre fra la direttiva ePrivacy e il RGPD: Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities - Adopted on 12 March 2019.

5. La bozza del nuovo regolamento

La bozza del 10 gennaio 2017 affronta l'esigenza di armonizzare la tutela dei dati personali nelle comunicazioni elettroniche alle nuove prospettive aperte dal RGDP. Di quest'ultimo infatti ne riprende l'impostazione e l'organizzazione, richiamandolo frequentemente in tutto il testo.
Sottolineate le seguenti definizioni:
I **dati** delle comunicazioni elettroniche (c.e.) sono composti da:

- **contenuto** delle c.e.: quello scambiato attraverso i servizi di c.e. quale testo, voce, video, immagini e suono;
- **metadati** delle c.e.: i dati associati al contenuto quali la fonte e il destinatario di una comunicazione, la localizzazione del dispositivo, la data, l'ora, la durata e il tipo di comunicazione,

si fissano le seguenti le finalità:

- tutelare i diritti e le libertà fondamentali delle persone fisiche e giuridiche e garantire la libera circolazione dei dati delle comunicazioni elettroniche e dei servizi di comunicazione elettronica nell'Unione,

e gli ambiti di applicazione:

- i trattamenti dei dati delle comunicazioni elettroniche effettuato in relazione alla fornitura e alla fruizione dei servizi di comunicazione elettronica e le informazioni connesse alle apparecchiature terminali degli utenti finali;
- i trattamenti effettuati in Europa, direttamente o indirettamente tramite rappresentante;
- i trattamenti connessi a servizi accessibili al pubblico.

Il CAPO II (artt. 5 – 11) rappresenta il cuore del trattamento:

- I dati delle c.e. sono riservati e vietate tutte le interferenze con i dati delle comunicazioni elettroniche, quali ascolto, registrazione, conservazione, monitoraggio, scansione o altri tipi di intercettazione, sorveglianza o trattamento dei dati delle comunicazioni elettroniche, da parte di persone diverse dagli utenti finali;
- Il trattamento del contenuto delle c.e. dei dati può essere effettuato esclusivamente con il consenso degli interessati;
- Il trattamento dei metadati delle c.e. può essere effettuato da parte del fornitore per esigenze di fatturazione o previo consenso

dell'interessato;
- Il trattamento dei dati delle c.e. può essere effettuato esclusivamente per l'espletamento del servizio di comunicazione;
- La cancellazione dei dati e dei metadati delle c.e. deve avvenire ad espletamento del servizio – salvo limitate esigenze tecniche. Il contenuto dei metadati necessario alla fatturazione segue l'iter amministrativo della stessa fatturazione;
- Vengono tutelate le stesse informazioni conservate nell'apparecchiatura terminale degli utenti finali;
- La gestione del consenso è ripresa completamente dall'articolo 7 del RGPD;
- Limitazioni dei diritti possono verificarsi per esigenze di salvaguardia degli interessi pubblici.

Il CAPO III (artt. 12 – 17) definisce una serie di obblighi da rispettare da parte del fornitore e di funzionalità che, opportunamente regolamentate, egli deve impegnarsi a mettere a disposizione dell'utente finale in modalità **gratuita**.
Si tratta di
- identificazione della linea chiamante e collegata;
- blocco delle chiamate in entrata;
- gestione degli elenchi pubblici;
- gestione delle comunicazioni indesiderate;
- informazioni agli utenti finali sui rischi reali o potenziali e sui possibili rimedi.

Nel seguito è interessante notare che la bozza del regolamento prende in considerazione le violazioni, dando le linee guida affinché possano essere applicate le sanzioni amministrative con importi ripartiti in due fasce (entro 10M€ o 20M€; 2% o 4% per le imprese) perfettamente simili al RGPD.
A conclusione vengono presentate delle scadenze (date di entrata in vigore e relative conseguenze – quali l'abrogazione della direttiva ePrivacy e clausole di monitoraggio) che, come anticipato, non sono state rispettate e per le quali si attendono aggiornamenti.

6 Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities - Adopted on 12 March 2019

In realtà questo documento è stato preceduto da una dichiarazione che l'EDPB ha ritenuto opportuno pubblicare il 25 maggio 2018, cioè lo stesso giorno in cui il nuovo regolamento ePrivacy sarebbe dovuto entrare in vigore, con l'obiettivo di mettere a disposizione un ulteriore contributo per la conclusione dell'iter di pubblicazione del nuovo regolamento.
Questa si può sintetizzare con le conclusioni :
Il Comitato europeo per la protezione dei dati ritiene che:
- *il regolamento ePrivacy non dovrebbe abbassare il livello di protezione offerto dall'attuale direttiva ePrivacy;*
- *il regolamento ePrivacy dovrebbe proteggere in modo neutrale dal punto di vista tecnologico tutti i tipi di comunicazioni elettroniche, compresi quelli effettuati dai servizi "Over-the-Top";*
- *il consenso dell'utente dovrebbe essere ottenuto sistematicamente in una maniera tecnicamente fattibile e vincolante prima*

del trattamento dei dati relativi alle comunicazioni elettroniche o prima di utilizzare le capacità di archiviazione o di elaborazione dell'apparecchiatura terminale dell'utente; non dovrebbero esservi eccezioni per trattare i dati in base al "legittimo interesse" del titolare del trattamento o al fine generico dell'esecuzione di un contratto;

- *l'articolo 10 (della bozza – ndr) dovrebbe prevedere un modo efficace per far sì che i siti web e le applicazioni mobili possano ottenere il consenso; più in generale, le impostazioni dovrebbero tutelare per impostazione predefinita la privacy degli utenti e questi dovrebbero essere guidati nella scelta di un'impostazione, a seguito della ricezione di informazioni pertinenti e trasparenti; a tale riguardo, il regolamento dovrebbe rimanere neutrale dal punto di vista tecnologico al fine di garantire che, indipendentemente dalle modalità di utilizzo, la sua applicazione rimanga coerente;*
- *dovrebbe essere applicato il più attento controllo possibile sulle eventuali eccezioni ad hoc che i legislatori potrebbero voler aggiungere a quelle già previste nelle bozze di testo della Commissione e del Parlamento. In particolare, qualsiasi eccezione formulata in termini generici per i casi in cui "un'autorità pubblica" richiede il trattamento dei dati dovrebbe essere esaminata con estrema attenzione, e la proposta non dovrebbe consentire il monitoraggio indiscriminato dell'ubicazione dell'utente o il trattamento dei suoi metadati;*
- *affinché il consenso sia fornito liberamente, come richiesto dal regolamento generale sulla protezione dei dati, l'accesso ai servizi e alle funzionalità non deve essere subordinato al consenso dell'utente al trattamento dei dati personali o al trattamento delle informazioni connesse alle apparecchiature terminali degli utenti finali, ossia i cookie wall devono essere espressamente proibiti;*
- *deve essere incentivato l'uso di dati di comunicazione elettronica resi effettivamente anonimi;*
- *i suddetti sviluppi tuteleranno la vita privata degli utenti finali in ogni contesto pertinente ed eviteranno qualsiasi distorsione della concorrenza.*

Si giunge quindi a marzo 2019 per la pubblicazione dell'Opinion 5/2019 con l'obiettivo di rispondere ai diversi quesiti sulle interazioni tra Direttiva ePrivacy e RGPD. Prende spunto da una richiesta dell'autorità garante belga finalizzata a richiedere al board chiarimenti su tale interazione.
La spiegazione pone in evidenza i tre argomenti trattati:

- problematiche di interesse del RGPD e non della direttiva;
- problematiche di interesse della direttiva e non del RGPD;
- problematiche che coinvolgono entrambi i provvedimenti.

Ci soffermiamo, per il particolare interesse che riveste, su quest'ultima condizione. Esempio:
"Se nel pubblicare o recuperare informazioni attraverso un cookie o un dispositivo simile, le informazioni raccolte possono essere considerate dati personali allora, oltre all'Articolo 5 (3) della direttiva ePrivacy, si applicherà anche la Direttiva 95/46/CE" (esempio formulato prima della promulgazione del RGPD).
Il RGPD aggiunge a questo proposito il considerando 30:
Le persone fisiche possono essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, marcatori temporanei (cookies) o identificativi di altro tipo, quali i tag di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle.
Ovviamente si vuole evitare un conflitto fra i diversi provvedimenti. A questo proposito l'EDPB suggerisce di applicare il principio ***lex specialis derogat generali***, cioè le disposizioni speciali prevalgono sulle norme generali. In altri termini, nelle situazioni in cui la direttiva ePrivacy "particolarizza" (ossia rende più specifiche) le regole del RGPD, le "specifiche" disposizioni della direttiva ePrivacy, in quanto lex specialis, prevalgono sulle "più generali" disposizioni del RGPD. Viceversa, qualsiasi trattamento di dati personali che non sia specificamente disciplinato dalla direttiva ePrivacy (o per la quale la direttiva ePrivacy non contiene una "regola speciale"), rimane soggetta alle disposizioni del RGPD.
Un esempio – tratto dal considerando 39 - che mostra come la direttiva ePrivacy "particolarizza" le disposizioni del RGPD può essere l'elaborazione dei cosiddetti "dati di traffico", come da art.6 della direttiva. In via ordinaria, il trattamento dei dati personali può essere giustificato sulla base di ciascuno dei motivi legittimi di cui all'articolo 6 del RGPD e dal considerando 49. Tuttavia, l'intera gamma di possibili motivi legittimi forniti dall'articolo 6 del RGPD non può essere applicato dal fornitore di un servizio di comunicazione elettronica all'elaborazione di dati sul traffico, in quanto l'articolo 6 della direttiva ePrivacy limita esplicitamente le condizioni in cui i dati sul traffico, compresi i dati personali, possono essere trattati. In questo caso, le disposizioni più specifiche della direttiva ePrivacy devono prevalere sulle disposizioni più generali del RGPD. L'arti-

colo 6 della direttiva ePrivacy non riduce tuttavia le richieste di altre disposizioni del RGPD, come i diritti dell'interessato né nega il requisito che il trattamento dei dati personali deve essere lecito, corretto e trasparente (art. 5 par.1 del RGPD).

7. European Data Protection Supervisor (EDPS) - Opinion 7/2020 on the Proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online

Durante il 2020 la Commissione ha adottato una strategia finalizzata alla lotta efficace nei confronti degli abusi sessuali sui minori. Questo fenomeno ha avuto enorme espansione nel corso dell'anno a causa della maggiore esposizione dei minori sulla rete provocata dai lunghi tempi di lockdown.

In particolare, il 10 settembre 2020 la Commissione ha pubblicato una proposta di regolamento provvisorio sul trattamento dei dati personali e di altro tipo ai fini della lotta all'abuso sessuale sui minori, che prevede una deroga temporanea all'articolo 5, paragrafo 1, e all'articolo 6 della direttiva ePrivacy. La deroga riguarda il trattamento dei dati personali in relazione alla fornitura di "servizi di comunicazione interpersonale indipendenti dal numero" (ad esempio, voice over IP, messaggistica e servizi di posta elettronica basati sul Web) (...), al solo scopo di rimuovere materiale pedopornografico e rilevare o segnalare gli abusi alle autorità di contrasto di tali reati.

A questo proposito l'EDPS (European Data Protection Supervisor) ha emanato l'Opinion 7/2020, in data 10 novembre 2020, che dà un giudizio di merito sulla proposta di regolamento alquanto critico.

"L'EDPS in particolare, osserva che le misure previste dalla proposta costituirebbero un'interferenza con i diritti fondamentali al rispetto della vita privata e alla protezione dei dati di tutti gli utenti di servizi di comunicazione elettronica molto popolari, come le piattaforme e le applicazioni di messaggistica istantanea. La riservatezza delle comunicazioni è una pietra angolare del diritto fondamentale al rispetto della vita privata e familiare.

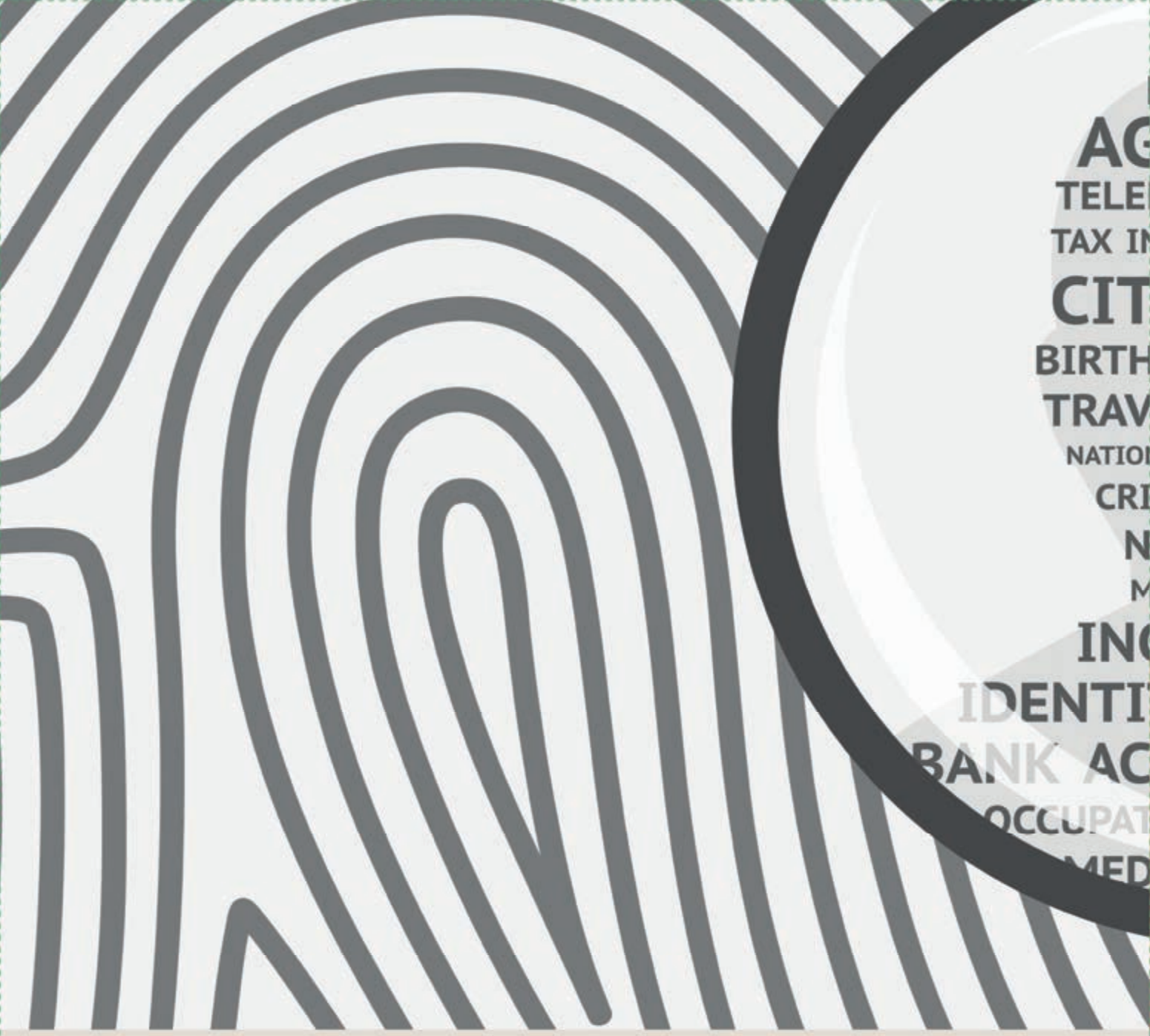
L'EDPS desidera sottolineare che le questioni in gioco non riguardano specificamente la lotta contro gli abusi sui minori, ma qualsiasi iniziativa volta alla collaborazione del settore privato a fini di applicazione della legge. Se adottata, la proposta costituirà inevitabilmente un precedente per la futura legislazione in questo settore. L'EDPS ritiene pertanto essenziale che la proposta ***non sia adottata****, anche sotto forma di deroga temporanea, fino a quando non saranno integrate tutte le necessarie garanzie previste nel presente parere.*

In particolare, nell'interesse della certezza del diritto, l'EDPS ritiene necessario chiarire se la proposta stessa è intesa a fornire o meno una base giuridica per il trattamento ai sensi del RGPD. In caso contrario, l'EDPS raccomanda di chiarire esplicitamente nella proposta quale base giuridica ai sensi del RGPD sarebbe applicabile in questo caso particolare. A questo proposito, l'EDPS sottolinea che gli orientamenti delle autorità di protezione dei dati non possono sostituire il rispetto del requisito di legalità. Il colegislatore deve assumersi la propria responsabilità e garantire che la deroga proposta sia conforme ai requisiti dell'articolo 15, paragrafo 1, secondo l'interpretazione della Corte di Giustizia Europea."

Come si vede, la direttiva ePrivacy rimane una norma dalla vita molto travagliata. Restiamo in attesa di aggiornamenti.

Sitografia:

1. La direttiva 2002/58/CE – ePrivacy
   https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/35284
2. La direttiva 2006/24/CE
   https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1485189
3. Sentenza della Corte (Grande Sezione) dell'8 aprile 2014
   https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:62012CA0293&from=FR
4. La direttiva 2009/136/CE
   https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1798132
5. La bozza del nuovo regolamento
   https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52017PC0010&from=EN
6. Dichiarazione sulla revisione del regolamento ePrivacy e sul suo impatto sulla tutela delle persone fisiche in relazione alla privacy e alla riservatezza delle loro comunicazioni
   https://edpb.europa.eu/our-work-tools/our-documents/drugi/statement-edpb-revision-eprivacy-regulation-and-its-impact_it
7. Opinion 5/2019 dell'edpb
   https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-52019-interplay-between-eprivacy-directive_it
8. Opinion 7/2020 dell'edps
   https://edps.europa.eu/sites/edp/files/publication/20-11-10_opinion_combatting_child_abuse_en.pdf



a cura di
Ing. Alessandro Alessandroni

GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI (DATA BREACH), PREVENZIONE E REAZIONE

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI ROMA

Introduzione

Il Regolamento Europeo GDPR attribuisce ai titolari del trattamento l'onere di adottare misure tecnico/organizzative atte a minimizzare la probabilità di violazione degli stessi dati (data breach) con conseguente possibile impatto sulle persone fisiche (interessati). Tali misure tecnico/organizzative[1], per quanto selezionate e applicate correttamente, non possono annullare del tutto la probabilità di un incidente e dunque il titolare è tenuto a mettere in atto un processo di gestione dei data breach che gli consenta di rendere minimo l'impatto sugli interessati dovuto ad una compromissione dei dati personali, ottemperando allo stesso tempo agli obblighi normativi previsti dallo stesso GDPR e da altre normative di settore.

L'articolo 33 del GDPR prevede la notifica all'autorità di controllo da parte del titolare del trattamento nel caso sia probabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche L'articolo 34 prevede anche la comunicazione all'interessato, nel caso il rischio per i diritti e le libertà delle persone fisiche sia elevato.

Indipendentemente dal fatto che una violazione debba o meno essere notificata all'autorità di controllo, il titolare del trattamento deve conservare in un Registro la documentazione di tutte le violazioni, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale Registro consente all'autorità di controllo di verificare il rispetto del Regolamento.
Conseguenze di un *data breach* per le organizzazioni possono essere il pagamento di sanzioni (comminate sulla base della normativa) ma anche il cosiddetto danno reputazionale.
Per adempiere a quanto richiesto dal GDPR i titolari e i responsabili del trattamento devono pianificare anticipatamente e mettere in atto processi per rilevare e limitare tempestivamente gli effetti di una violazione, valutare la gravità in termini di rischio per gli interessati e, se necessario, notificare la violazione all'autorità di controllo competente e comunicarla agli stessi interessati.

Definizione e tipi di violazione dei dati personali

All'articolo 4, punto 12, il regolamento definisce la "violazione dei dati personali" come "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".
Le violazioni possono essere classificate in base ai tre ben noti principi della sicurezza delle informazioni:

- "violazione della riservatezza", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;
- "violazione dell'integrità", in caso di modifica non autorizzata o accidentale dei dati personali;
- "violazione della disponibilità", in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.
- Una violazione può riguar dare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse.

Il processo di gestione dei data breach

Le violazioni dei dati personali sono incidenti di sicurezza informatica che riguardano dati personali. Il processo di gestione coincide, in gran parte, con il processo di gestione degli incidenti con in più l'iter relativo ai processi di notifica previsti dal GDPR (vedi figura 1[2]).
Presupposto per la corretta gestione dei *data breach* è che sia operativo un processo di monitoraggio e gestione degli incidenti di sicurezza informatica in linea con le norme tecniche internazionali quali la norma ISO/IEC 27035 "Information security incident Management" e la norma NIST SP-800-61 RV2 "Computer Security Incident Handling Guide"[3].
Tra gli strumenti a disposizione del team addetto alla gestione degli incidenti di sicurezza (CSIRT[4] o altro organismo analogo) particolare rilevanza hanno le piattaforme SIEM. La tecnologia dei sistemi SIEM ha come obiettivo la raccolta centralizzata dei log e degli eventi generati da applicazioni e sistemi in rete, per consentire agli analisti di sicurezza di ridurre i tempi necessari alla risoluzione e alle indagini su allarmi e incidenti di sicurezza.
Occorre pertanto predisporre le procedure, gli strumenti e l'organizzazione per gestire i *data breach* al meglio in stretta collaborazione con il CSIRT.
La procedura di notifica relativa al *data breach* viene attivata da una segnalazione di un *data breach* al titolare o a un suo designato per la gestione.
Da questo momento, parallelamente all'analisi dell'incidente e alle azioni di contenimento e di eventuale recovery[5] previste per gli incidenti di sicurezza svolte dal CSIRT, viene avviata, da parte del titolare o di un suo designato, la valutazione della gravità della violazione dei dati (*Data Breach Severity*) in termini di rischi per i diritti e per le libertà degli interessati.

Figura 1

Se l'esito della valutazione comporta la notifica al Garante del *data breach*, occorre compilare il modulo di notifica e trasmetterlo entro 72 ore dall'accertamento del *data breach*.
Nel caso l'esito della valutazione comporti anche la comunicazione agli interessati, occorre compilare il modulo di comunicazione e trasmetterlo o diffonderlo appena possibile[6].
Il sottoprocesso si conclude con l'aggiornamento del registro dei *data breach*, disponibile per eventuale consultazione da parte del Garante.

Valutazione della gravità del Data Breach (rischio per gli interessati)
Sussiste un rischio per gli interessati quando la violazione può comportare un danno fisico, materiale o immateriale per le persone fisiche i cui dati sono stati violati. Esempi di tali danni sono la discriminazione, il furto o l'usurpazione d'identità, perdite finanziarie e il pregiudizio alla reputazione.
Il verificarsi di tale danno dovrebbe essere considerato probabile quando la violazione riguarda dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, oppure che includono dati genetici, dati relativi alla salute o dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza.
Nella valutazione del rischio si dovrebbero prendere in considerazione tanto la probabilità quanto la gravità del rischio per i diritti e le libertà degli interessati. Inoltre, il regolamento afferma che il rischio dovrebbe essere valutato in base a una valutazione oggettiva.
Se è stata effettuata una valutazione di impatto dei rischi del trattamento dei dati personali (DPIA) si possono utilizzare i risultati di questa analisi adattandoli al contesto specifico del *data breach* in esame.
Le "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679" versione 6.02.2018[7], redatto dal

SE < 2	LOW	Gli individui non saranno interessati o potrebbero incontrare alcuni inconvenienti, che supereranno senza alcun problema (tempo trascorso a reinserire informazioni, fastidi, irritazioni, ecc.).
2 ≤ SE < 3	MEDIUM	Gli individui possono incontrare notevoli disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici minori, ecc.).
3 ≤ SE< 4	HIGH	Gli individui possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, lista nera da parte delle banche, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).
4 ≤ SE	VERY HIGH	Gli individui possono incontrare conseguenze significative, o addirittura irreversibili, che non possono superare (difficoltà finanziarie come debito sostanziale o incapacità lavorativa, disturbi psicologici o fisici a lungo termine, morte, ecc.).

Figura 2

Gruppo di Lavoro Articolo 29 per la Protezione dei Dati Personali indicano i fattori principali da prendere in considerazione:

- tipo di violazione;
- natura, caratteristiche di sensibilità e volume dei dati personali;
- facilità di identificazione delle persone fisiche;
- gravità delle conseguenze per le persone fisiche;
- caratteristiche particolari dell'interessato e del titolare del trattamento;
- numero di persone fisiche interessate.

Per garantire la oggettività della valutazione della gravità della violazione dei dati e il corrispondente livello di rischio per i diritti e le libertà degli interessati, è possibile utilizzare la metodologia elaborata dall'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA)[8], suggerita dalle citate Linee Guida del GdL Art. 29.

Tale metodologia prevede che il calcolo della gravità del Data Breach venga effettuato sulla base di tre fattori:

- **Contesto di elaborazione dei dati** (DCP): valutato sulla base del tipo di dati coinvolti nel *data breach* e di fattori di correzione relativi al contesto, che aumentano la criticità della violazione anche nel caso di dati "semplici"; può valere da 1 a 4;
- **Facilità di identificazione** (EI): valutato sulla base dei dati personali coinvolti nel *data breach*; è un fattore correttivo di DCP con valori da 0,25 a 1;
- **Circostanze della violazione** (CB): valutato in base alle tipologie di *data breach* e alla eventuale intenzionalità della violazione; CB è un fattore additivo che può variare da 0 a 2, nel caso estremo di violazione intenzionale che impatti su riservatezza, disponibilità e integrità.

Il calcolo della gravità (SEverity) si effettua con la formula SE = DCP x EI + CB. Il livello di gravità viene associato al valore SE secondo una scala a quattro livelli riportata nella tabella illustrata in figura 2.

Gli obblighi di notifica all'Autorità di Controllo scaturiscono dal superamento di una soglia di rischio basso (art. 33 del GDPR) mentre l'obbligo di comunicazione agli interessati è innescato dal superamento di un rischio elevato per le libertà e i diritti degli interessati (art. 34 del GDPR). La metodologia fornisce soltanto un supporto al titolare al quale spetta la decisione in merito alla necessità o meno di procedere alla notifica al Garante e alla comunicazione agli interessati.

Notifica al Garante Privacy

Una volta valutata la necessità di effettuare la notifica della violazione dei dati subita, il titolare del trattamento o un suo designato provvederà, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, ad effettuare la notifica utilizzando il modello proposto dal Garante nel Provvedimento del 30.07.2019[9] che si compone delle sezioni indicate nella tabella 1.

Se la gravità della violazione è stata valutata utilizzando il tool basato sulla metodologia ENISA è opportuno indicarlo nella sezione E.

Si noti che nella notifica devono essere indicate in dettaglio le misure tecniche organizzative presenti e quelle adottate a seguito della violazione. È pertanto opportuno non solo adottare misure di sicurezza adeguate al rischio ma anche mantenere documentazione aggiornata da allegare alla notifica.

La notifica deve essere inviata al Garante trami-

• TIPO DI NOTIFICA (preliminare, completa, integrativa)
• SEZ.A **Dati** del soggetto che effettua la notifica
• SEZ. B **Titolare del Trattamento**
• SEZ. B1 **Dati di contatto** per informazioni relative alla violazione (Responsabile Protezione Dati personali o altro soggetto)
• SEZ. B2 **Ulteriori soggetti coinvolti** nel trattamento (Contitolare, Responsabile del trattamento...)
• SEZ. C **Informazioni di sintesi sulla violazione** (data della violazione e di scoperta, natura, causa, categorie di dati personali coinvolti e categorie di interessati, numero di interessati coinvolti)
• SEZ. D **Informazioni di dettaglio** sulla violazione o descrizione incidente di sicurezza alla base della violazione o descrizione categorie di dati personali oggetto della violazione o sistemi e infrastrutture IT coinvolti o misure tecniche e organizzative adottate per la sicurezza dei dati dei sistemi e delle infrastrutture IT coinvolte
• SEZ. E **Possibili conseguenze per gli interessati e gravità della violazione**
• SEZ. F **Misure adottate a seguito della violazione** o per porre rimedio e ridurre effetti negativi o per prevenire simili violazioni future
• SEZ. G **Comunicazione agli interessati**
• SEZ. H Altre informazioni (altri paesi coinvolti, notifiche ad altre autorità)

Tabella 1

te posta elettronica certificata all'indirizzo protocollo@pec.gpdp.it oppure tramite posta elettronica ordinaria all'indirizzo protocollo@gpdp.it e deve essere sottoscritta digitalmente (con firma elettronica qualificata/firma digitale) ovvero con firma autografa.
Le notifiche al Garante effettuate oltre il termine delle 72 ore devono essere accompagnate dai motivi del ritardo.

Notifica in più fasi

Il regolamento prende atto del fatto che il titolare del trattamento non sempre dispone di tutte le informazioni necessarie su una violazione entro 72 ore dal momento in cui ne è venuto a conoscenza, dato che non sempre sono disponibili entro tale termine dettagli completi ed esaustivi su un incidente.
È possibile effettuare la notifica in più fasi quando il titolare del trattamento ha la necessità di effettuare ulteriori accertamenti per stabilire tutti i fatti pertinenti relativi all'incidente.
L'articolo 33, paragrafo 4, del GDPR afferma: "Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo".

Comunicazione agli interessati

Una volta valutata la necessità di effettuare la comunicazione della violazione dei dati agli interessati, sulla base della procedura di cui allo step 3, secondo quanto prescritto dal Regolamento (UE) 2016/679, il titolare o un suo designato dovrà provvedere, senza indebito ritardo.
Quanto al contenuto di tale comunicazione, il GDPR afferma che la comunicazione deve contenere almeno:

- natura della violazione;
- nome e dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- descrizione delle possibili conseguenze della violazione dei dati personali;
- descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e per attenuare i possibili effetti negativi.

La comunicazione agli interessati dovrà essere scritta in un linguaggio chiaro e semplice.
Quanto alle modalità di comunicazione, caso per caso, il titolare dovrà sempre privilegiare la modalità di comunicazione diretta con i soggetti interessati (quali email, SMS o messaggi diretti).
Nel caso in cui la segnalazione diretta richieda uno sforzo ritenuto sproporzionato, allora si potrà utilizzare una comunicazione pubblica, che dovrà essere ugualmente efficace nel contatto diretto con l'interessato.

Attività post-incidente: Inserimento dell'evento nel Registro delle Violazioni

Il titolare del trattamento o un suo designato, con il supporto dei Responsabili del trattamento, deve documentare le violazioni di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati (si veda art. 33, paragrafo 5).
Il Registro dei *data breach* deve essere continuamente aggiornato e messo a disposizione del Garante, qualora l'Autorità chieda di accedervi.
Nelle citate linee guida predisposte dal WP29 si forniscono le seguenti indicazioni in merito ai dati da registrare.

- dettagli delle violazioni:

- descrizione di ciò che è avvenuto;
- cause;
- dati personali interessati (tipo e numero);
- effetti e conseguenze della violazione;
- azioni correttive adottate;
- motivazioni per violazioni non notificate/comunicate o notificate/comunicate in ritardo.

Le violazioni dei dati sono quasi molto spesso sintomi di vulnerabilità presenti. È quindi necessario verificare se vulnerabilità che hanno dato origine all'incidente sono ancora presenti e se è possibile rimuoverle per evitare che possano essere la causa di ulteriori attacchi.
È inoltre opportuno tenere una riunione di "lezioni apprese" con tutte le parti coinvolte dopo un *data breach*, specialmente se di grave entità, per migliorare le misure di sicurezza e il processo di gestione dell'incidente stesso.

Note:

1 Oltre alle misure di sicurezza previste dalle norme ISO/IEC 27001-2 o dal Framework Nazionale per la sicurezza informatica, utili indicazioni sulle misure da adottare per prevenire o attenuare i rischi di una potenziale violazione dei dati sono contenute nelle recenti Linee guida, adottate dall'Edpb (Comitato europeo per la protezione dei dati) https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf
2 Dalla "Guide on personal data breach management and notification", della Agencia Espanola de protection de datos, https://www.aepd.es/sites/default/files/2019-09/Guide-on-personal-data-breach.pdf
3 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
4 Computer Security Incident Response Team.
5 Azioni che possano limitare i danni che la violazione potrebbe causare (i.e. riparazione fisica di strumentazione; utilizzo dei file di back up per recuperare dati persi o danneggiati; isolamento/chiusura di un settore compromesso della rete; cambio dei codici di accesso; ecc.); le decisioni sulle azioni di contenimento da intraprendere sono facilitate dalla presenza di strategie e procedure di contenimento predefinite per i principali tipi di data breach.
6 Il GDPR non pone un termine definito ma richiede che la comunicazione avvenga "senza giustificato ritardo".
7 https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49827
8 https://www.enisa.europa.eu/publications/dbn-severity/at_download/fullReport
9 https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9126951

CHECKING
NETWORK
CONNECTED
[PROCESSING]
//SCAN
NETWORK
[PROCESSING]
02
//HACK ATTEMPT FAILED
[PROCESSING]
USER SAFE
//SCAN
12.123.8234

GDPR

LA DPIA DATA PROTECTION IMPACT ASSESSMENT

Introduzione

Sono passati quasi tre anni dal maggio 2018, quando il Regolamento sulla protezione dei dati personali (GDPR) è diventato operativo. In questo periodo tante problematiche sui concetti innovativi che il GDPR ha espresso sono state oggetto di confronto e chiarimenti; tante altre rimangono ancora aperte o soggette ad ulteriori indagini di interpretazione e approfondimenti.

Uno degli argomenti su cui si è particolarmente dibattuto, e che continua ad essere oggetto di aggiornamento da parte dei Garanti per la Protezione dei dati personali sia europeo che dei singoli paesi UE, è la DPIA - Data Protection Impact Assessment.

a cura di
Ing. Natale Castelliti

Quando effettuare la DPIA

La DPIA è lo strumento con il quale il Regolamento assegna la responsabilità al Titolare nel decidere se il trattamento è suscettibile di rischio. Il primo comma dell'articolo 35 recita: *"Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali."*

Al fine di decidere il grado di esposizione al rischio del trattamento e conseguentemente l'opportunità di svolgere una DPIA, viene in aiuto il documento WP248 dello European Data Protection Board (ex Working Party) nella versione emendata ed adottata il 4 ottobre 2017.

Questo suggerisce di prendere in considerazione i seguenti nove criteri:

1. Trattamenti valutativi o di scoring, compresa la profilazione e attività predittive;
2. Decisioni automatizzate che producono significativi effetti giuridici o di analoga natura;
3. Monitoraggio sistematico;
4. Dati sensibili o dati di natura estremamente personale;
5. Trattamenti di dati su larga scala;
6. Combinazione o raffronto di insiemi di dati;
7. Dati relativi a interessati vulnerabili;
8. Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;
9. Tutti quei trattamenti che, di per sé, "impediscono [agli interessati] di esercitare un diritto o di avvalersi di un servizio o di un contratto".

Nella maggioranza dei casi un Titolare del trattamento dei dati personali può ritenere opportuno svolgere una DPIA quando almeno due delle casistiche sopra esposte vengono soddisfatte.

Il WP248 viene ripreso e ulteriormente chiarito dal Garante per la Protezione dei Dati Personali (GPDP) nel documento "Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679" dell'11 ottobre 2018.

In un processo di DPIA il titolare del trattamento o il responsabile del trattamento dovrebbero consultarsi con il RPD – Responsabile per la Protezione dei Dati - fra l'altro, sulle seguenti tematiche (da: Applicare il GDPR - Le linee guida europee - 2019 - del GPDP):

- se condurre o meno una DPIA;
- quale metodologia adottare nel condurre una DPIA;
- se condurre la DPIA con le risorse interne ovvero esternalizzandola;

- quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e gli interessi delle persone interessate;
- se la DPIA sia stata condotta correttamente o meno, e se le conclusioni raggiunte (procedere o meno con il trattamento e quali salvaguardie applicare) siano conformi ai requisiti in materia di protezione dei dati.

Come effettuare una DPIA

Effettuare una DPIA significa implementare un'analisi del rischio. Si possono adottare diverse tecniche, qualitative e quantitative, al fine di valutare il rischio in un processo sotto l'aspetto della protezione del dato personale trattato. Nel corso di questi anni sono stati proposti ed adottati diversi modelli di DPIA da parte di aziende private e pubbliche, modelli utilizzati per la conduzione dell'assessment sia all'interno che verso società terze. È interessante notare che il GPDP pubblicizza un software messo a disposizione dal CNIL (il GPDP francese) e tradotto anche in italiano. È un software semplice da usare, utile per realtà non molto complesse; ha avuto diversi aggiornamenti nel tempo.

Uno dei metodi tradizionali più comuni è l'FMEA, Failure Mode and Effect Analysis (Analisi dei modi e degli effetti dei guasti). Questo strumento permette di valutare il rischio come prodotto di tre indici:

Severità	Stima della gravità di un evento, opportunamente indicizzata e misurabile
Occorrenza	Stima della frequenza possibile di accadimento, opportunamente indicizzata e misurabile
Rilevabilità	Stima della capacità del sistema di rilevare un evento rischioso e farvi fronte.

Definito lo strumento, si passa ad identificare le categorie degli eventi che rappresentano un potenziale rischio per il trattamento in oggetto. Questa fase è fortemente collegata agli aspetti precipui del trattamento, del contesto aziendale, delle persone e loro formazione, ecc. Gestire l'elenco dei clienti di un laboratorio di analisi o di un'azienda di apparecchiature biomediche potrebbe essere più complesso e rischioso dell'anagrafe degli iscritti di una palestra. Ad ogni modo per avere un supporto nella definizione della tassonomia degli eventi di rischio, è consigliabile ricondursi a standard riconosciuti da cui poi dettagliare i singoli eventi caso per caso. Uno dei metodi particolarmente efficaci nel definire in maniera completa ed esaustiva le casistiche da prendere in considerazione sono le Dichiarazioni di Applicabilità (Statement of Applicability – SOA) nelle appendici A e B del nuovo standard ISO/IEC 27701:2019 (Estensione degli standard ISO 27001 e ISO 27002 alla gestione delle informazioni riguardanti la privacy).

Queste riprendono le SOA della ISO 27001 ma con particolare attenzione alle problematiche della protezione dei dati personali, fino al punto che i controlli vengono suddivisi fra quelli da applicare come titolare del trattamento (Appendice A) e quelli da applicare come responsabile (Appendice B).
In tabella 1 viene presentata un elenco estratto da una possibile tassonomia di aree/funzioni investigate che si possono ricondurre a sei processi che ne formano una sintesi. Ad ogni riga può essere associato uno o più eventi potenzialmente rischiosi da valutare con la tripletta di indici definiti sopra. In figura 1 si presenta uno spaccato di uno studio sul trattamento dei dati gestiti dal ciclo attivo di un Customer Service.
Calcolata la media dei rischi per processo, se ne può presentare una sintesi con un diagramma spider come in figura 2. La linea azzurra rappresenta lo stato di rilevazione iniziale, quella rossa uno stadio intermedio o finale che tenga conto di un processo di gap analisi e piano di rientro. Occorre sottolineare che l'analisi e l'abbattimento del rischio tengono conto dell'evoluzione dell'organizzazione: si tratta, quindi, di un processo dinamico.
In questa fase si cerca di rilevare opportuni attributi che possano descrivere bene il rischio che si sta trattando al fine di poterlo affrontare meglio, catalogare, quantificare. Ad esempio, si definisce quali sono le funzioni aziendali impattate, chi potrebbe essere il responsabile dell'attività di rientro, se il rischio è di origine interna all'organizzazione o esterna ed altro ancora.

Consultazione preventiva per la valutazione d'impatto sulla protezione dei dati

In figura 3 viene presentato il tipico andamento qualitativo del rientro del rischio nel corso degli investimenti ad esso dedicati. In fase di rientro, il livello di sicurezza aumenta velocemente a fronte dei primi investimenti (smart goal). Con il crescere degli investimenti si riduce progressivamente il valore incrementale del livello di sicurezza raggiunto, fino a rendersi inutilmente oneroso. La scelta del punto in cui fermarsi con gli investimenti ricade esclusivamente sul management aziendale. Chi è abituato a gestire progetti di sicurezza identifica, di solito, il trade off nel punto in cui il costo della sicurezza eguaglia quello del rischio.
In situazioni particolarmente complesse può succedere che sia tecnicamente difficile o oneroso abbassare il rischio a livelli ragionevoli. Nel caso in cui il rischio residuo non dovesse essere giudicato sufficientemente basso da rientrare nei

Processo	Funzione investigata
Flusso Trattamento	Acquisizione dato
Flusso Trattamento	Destinazione dato
Flusso Trattamento	Storage
Flusso Trattamento	Backup
Flusso Trattamento	Cancellazione dato
Flusso Trattamento	Dati gestiti all'esterno
Flusso Trattamento	Flussi di dati extra UE
Flusso Trattamento	Dati su internet
Flusso Trattamento	Log di sistema
Documentazione Privacy	Finalità
Documentazione Privacy	Informativa
Documentazione Privacy	Consenso
Documentazione Privacy	Nomine a Responsabile / Persona autorizzata al trattamento dei dati personali / DPO / Rappresentante
Documentazione Privacy	Nomina ad Amministratore di sistema
Documentazione Privacy	Procedure aziendali riguardanti privacy e sicurezza fisica e informatica
Documentazione Privacy	Crisi / Data breach

Tabella 1

Asset	Sicurezza fisica delle sedi dove viene effettuato il trattamento
Asset	Infrastrutture di sede
Asset	Rete e trasmissione dati
Asset	Dispositivi portatili
Asset	Software
Asset	Sito web
Asset	Licenze
Asset	Ciclo di vita del cartaceo
Fornitore	Servizi di sede (office automation, guardiania, pulizie, manutenzioni…)
Fornitore	Infrastrutture in cloud
Fornitore	Dispositivi portatili
Fornitore	Rete e trasmissione dati
Fornitore	Software
Fornitore	Consulenti (medici, consulenti del lavoro, auditor, …)
Accessi ai sistemi	Autenticazione (standard o strong)
Accessi ai sistemi	Autorizzazione utenze per ruoli
Accessi ai sistemi	Accesso di terze parti ai sistemi dell'organizzazione
Risorse umane	Formazione per la protezione dati personali per i responsabili e gli incaricati
Risorse umane	Assenza del personale

Tabella 1

limiti di accettabilità, il GDPR prevede una fase di "consultazione preventiva" con il Garante, al fine di riceverne una consulenza sulla modalità di procedere nella situazione ritenuta a rischio. Il Garante ha l'obbligo di dare risposta scritta alla richiesta entro 8 settimane, prorogabili di ulteriori 6 settimane in caso di particolare complessità del tema proposto; il suo parere è vincolante.

Conclusioni

L'analisi di impatto e la consultazione preventiva rappresentano un cambiamento fondamentale nel trattamento del rischio nell'ambito della protezione dei dati personali. La DPIA non è un documento formale né statico ma una base di confronto che coinvolge diversi attori di un'azienda costringendoli a riflettere sull'esposizione ai rischi nell'ambito dei dati personali, così come già avviene in altri ambiti particolarmente critici. È un documento che è alla base dell'accountability richiesta al titolare dal GDPR e che va aggiornato frequentemente per non perdere di efficacia.
Non pochi assessment sono stati rivisti di recente perché non prendevano in considerazione l'evento pandemico e i suoi effetti devastanti, in quanto ritenuto a bassissima probabilità di accadimento. È un esempio quanto mai attuale per dimostrare la validità e la vitalità di questo strumento.

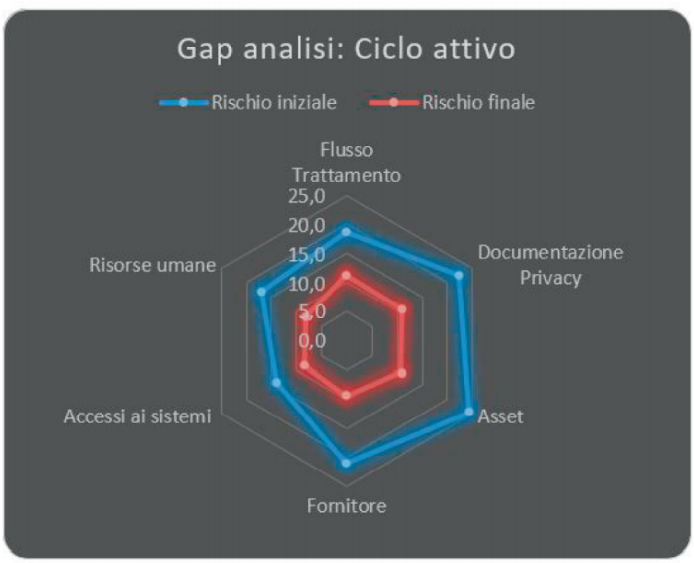


Figura 2

Analisi di impatto
Trattamento: Flusso delle

Item #	Processo	Input	Rischio potenziale	Azioni che provocano rischio						Diritti violabili					
#	Processo	Funzione investigata		Uso scorretto	Danno	Spionaggio	Perdita	Modificazione	Superamento dei limiti	Diritto alla privacy	Libertà di espressione e pensiero	Dati non essere discriminati	Diritto alla libertà di coscienza e religione	Libertà di movimento	Diritti dell'interessato
1	Flusso Trattamento	Acquisizione dato	Furto, perdita, alterazione, errore del dato fornito	x	x	x	x	x		x		x	x		x
2	Flusso Trattamento	Destinazione dato	Errore nel contenuto, consegna sbagliata	x	x		x	x		x	x	x	x	x	x
3	Flusso Trattamento	Storage	Danno generico in fase di utilizzo; malfunzionamento	x	x	x	x	x	x	x		x	x		x
4	Flusso Trattamento	Backup	Frequenza, conservazione, test	x	x	x	x	x		x	x	x	x	x	x
5	Flusso Trattamento	Cancellazione dato	Non effettuata, non controllata	x		x	x			x	x	x	x	x	x
6	Flusso Trattamento	Dati gestiti all'esterno	Flusso non controllato, non formalizzato	x	x	x	x	x		x	x	x	x	x	x

Figura 1

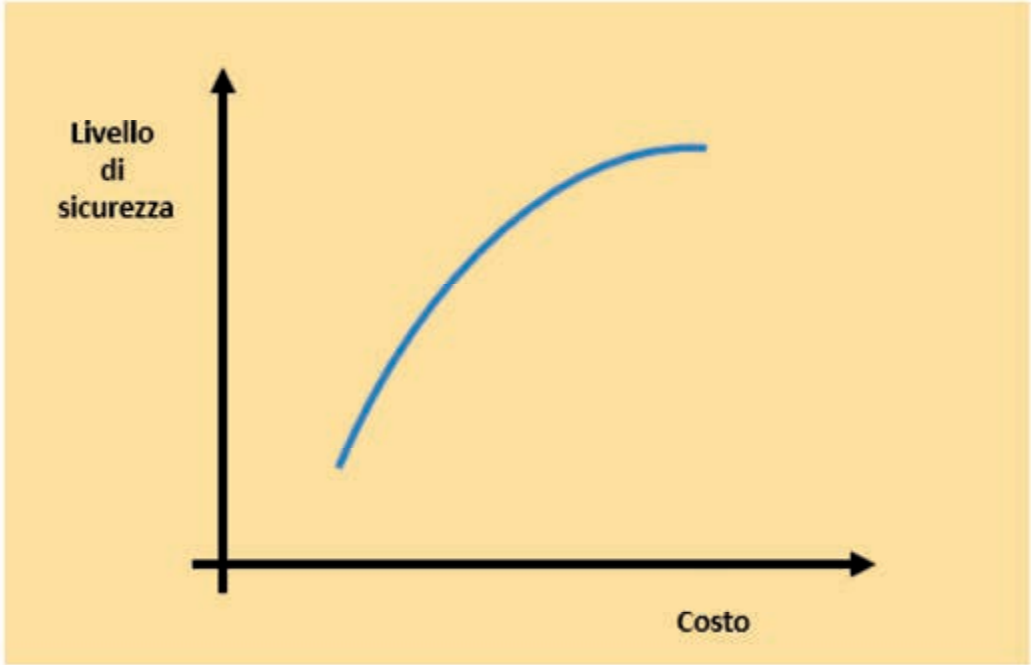
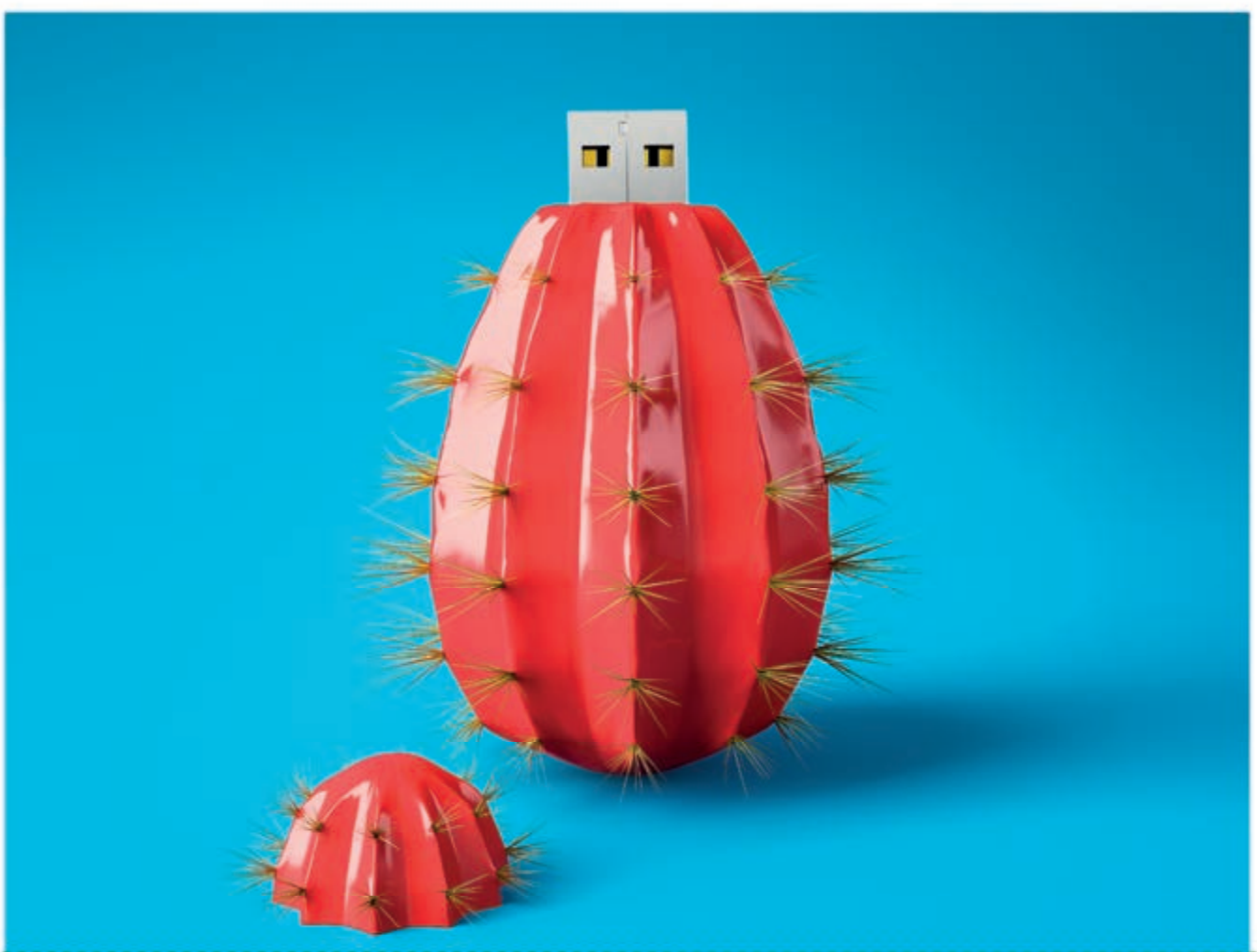


Figura 3

sui dati personali
applicazioni del ciclo attivo

Severità	Possibilità di accadimento	Valutazione assessment	VAS	RIS	Azione raccomandata	SCE	Sev	Acc	Vas 2	Rischio residuo	Rischio residuo accettato?
0-6	0-1	Giustificazione dello score assegnato	0-5								S / No
4	1	Possibili difetti di imputazione; errori di dati incontrollati; spionaggio	2	8			4	1	2	8	si
6	1	Rischio basso essendo automatizzato	1	6			6	1	1	6	si
4	1	Considerando la quantità degli applicativi utilizzati per il trattaento si deduce un'alta esposizice al rischio	4	16	Misura dello storico degli eventi di danno o malfunzonamento e creazione di una procedura di gestione degli storage per azioni di prevenzione		4	1	2	16	no
6	1	Esiste una data retention policy che indica una buona gestione dei backup ma non vengono indicate tutte le applicazioni soggette a backup	3	18	Migliorare la policy di backup con una completa descrizione delle modalità di backup degli applicativi che utilizzano il trattamento	x	6	1	2	12	no
6	1	Esiste una policy che indica il periodo di data retention dei dati sui backup ma non vengono indicate tutte le applicazioni che effettuano il trattamento	3	18	Migliorare la policy di data retention con una completa descrizione degli applicativi che utilizzano il trattamento	x	6	1	2	12	
6	1	Si ha evidenza di sistemi di controllo su quasi tutti gli applicativi del trattamento	2	12	Verificare i rimanenti applicativi del trattamento e implementare un sistema di data loss prevention	x	6	1	2	12	



ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI ROMA
Piazza della Repubblica, 59 - 00185 - Roma

Tel. 06.487.93.11 - Fax: 06.487.931.223
Cod.Fisc. 80201950583

Orari di apertura al pubblico degli uffici

Lunedì	09:30-12:30	14:30-17:30
Martedì	09:30-12:30	14:30-17:30
Mercoledì	09:30-12:30	14:30-17:30
Giovedì	09:30-12:30	14:30-17:30
Venerdì	09:30-12:30	chiuso
Sabato	chiuso	

La Segreteria dell'Ordine chiude alle 16.00

AREE DEL SITO WEB DEL QUADERNO

AREA CIVILE AMBIENTALE
https://rivista.ording.roma.it/civile/

AREA INDUSTRIALE
https://rivista.ording.roma.it/industriale/

AREA DELL'INFORMAZIONE
https://rivista.ording.roma.it/informazione/

AREA INTERSETTORIALE
https://rivista.ording.roma.it/intersettoriale/

È possibile consultare tutti i numeri
all'indirizzo Internet
ioroma.info

Quaderno Speciale

La Sicurezza Informatica per la protezione dei dati

Ordine degli Ingegneri della Provincia di Roma
Piazza della Repubblica, 59 - 00185 Roma
www.ording.roma.it