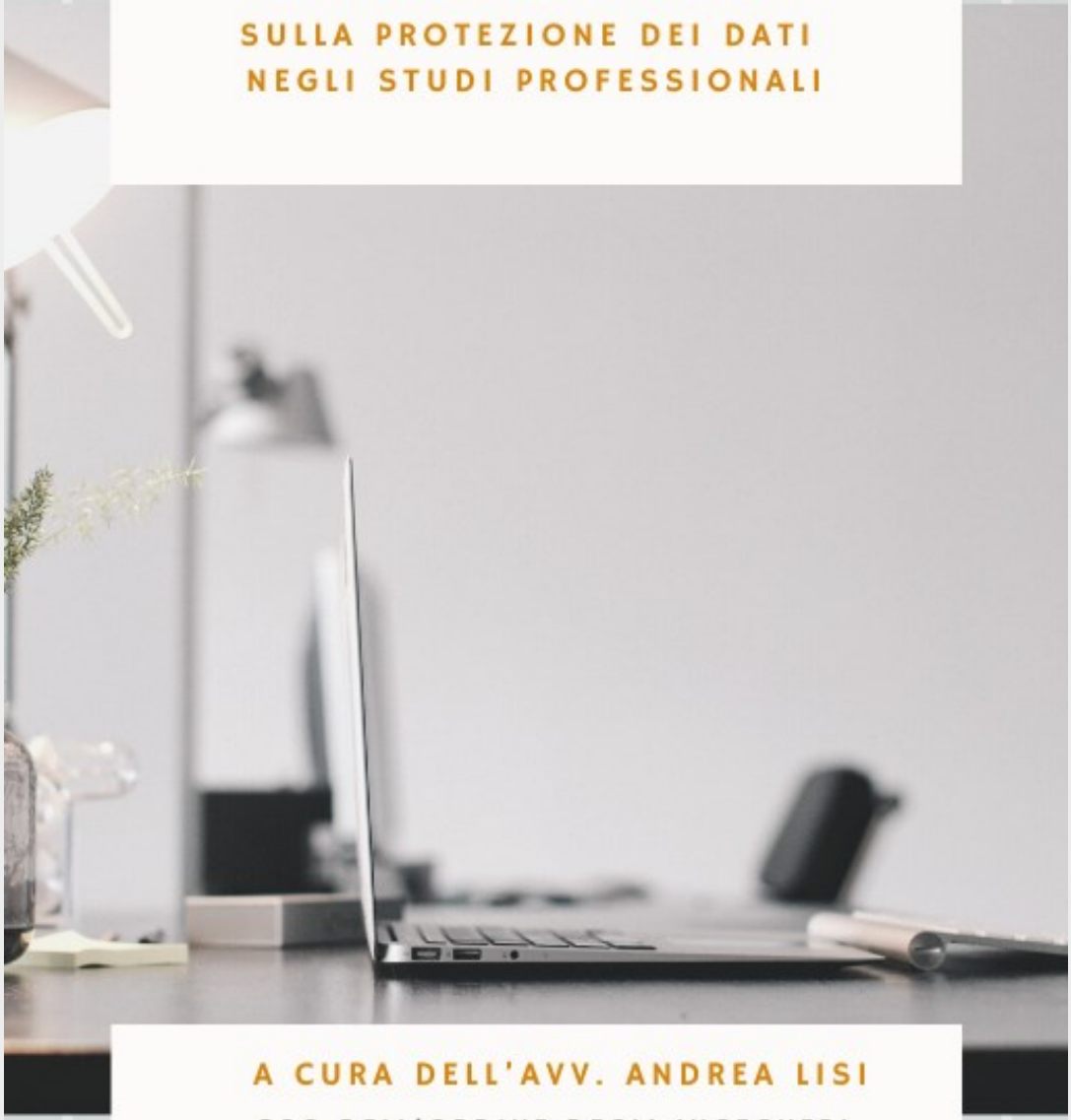
VADEMECUM

SULLA PROTEZIONE DEI DATI NEGLI STUDI PROFESSIONALI



A CURA DELL'AVV. ANDREA LISI

DPO DELL'ORDINE DEGLI INGEGNERI
DELLA PROVINCIA DI LECCE

ordine ingegneri provincia di lecce

Il presente Vademecum contiene la descrizione delle procedure e misure di sicurezza tecniche e organizzative da adottare all'interno degli Studi professionali, alla luce delle disposizioni del Regolamento Europeo n. 679/2016 (General Data Protection Regulation – GDPR), del D.Lgs. n. 196/2003 (Codice in materia di protezione dei dati personali), dei provvedimenti dell'Autorità Garante per la protezione dei dati personali e dell'European Data Protection Board (ex WP 29).

Il Vademecum è a cura dell'Avv. Andrea Lisi, DPO dell'Ordine degli Ingegneri di Lecce.

Hanno collaborato alla stesura i componenti del Team del DPO:

Avv. Sarah Ungaro

Avv. Mario Montano

Avv. Carola Caputo

Il presente documento è stato espressamente realizzato per l'Ordine degli Ingegneri di Lecce.

Lecce, 3 marzo 2021

Sommario

Premesse

Il principio di *accountability*, introdotto dal GDPR, comporta per qualsiasi organizzazione - compresi gli Studi professionali – una necessaria e approfondita auto-analisi sia della modalità di circolazione (interna ed esterna) dei dati personali (e quindi delle procedure adottate per ritenere tali trattamenti conformi alla normativa), che delle specifiche misure di sicurezza tecniche e organizzative messe in atto. È inoltre necessario monitorare la correttezza delle procedure di trattamento e protezione dei dati personali, soprattutto sotto il profilo giuridico, oltre che tecnico-informatico.

Si precisa in proposito che occorre distinguere tra il modello organizzativo di assessment per la protezione del dato – da finalizzare attraverso una metodologia di analisi prevalentemente organizzativa e di controllo – e lo sviluppo di politiche di sicurezza informatica a protezione del patrimonio informativo e documentale. In ottica GDPR, queste ultime devono essere soppesate in base a un'indispensabile analisi preventiva, che tenga conto della tipologia dei dati trattati e dei rischi reali che corrono gli stessi database e archivi.

In particolare, per essere *compliant* rispetto alle norme del GDPR, non sarà più sufficiente adottare un approccio meramente formalistico, che si traduceva sino a oggi, nella maggior parte dei casi, nella svogliata adozione delle misure minime di sicurezza di cui all'Allegato B (disciplinare tecnico, ormai abrogato) del D.Lgs. 196/2003, nella redazione di informative e nomine a responsabili e incaricati e nell'acquisizione dei consensi degli interessati, ove necessario.

Nel nuovo scenario normativo infatti, che delinea un approccio di *accountability* (ovvero di "responsabilizzazione") il titolare del trattamento deve porre in essere tutte le misure di sicurezza in termini sì tecnologici, ma soprattutto organizzativi, adeguate a dimostrare (e documentare) di aver improntato i trattamenti di dati personali anche ai principi della privacy *by design* e alla privacy *by default* (a mero titolo esemplificativo: istituendo e alimentando correttamente il registro dei trattamenti; adottando una procedura per analizzare i rischi di ogni trattamento e quindi decidere se effettuare un *Privacy Impact Assessment*; verificando che l'archiviazione dei dati personali nelle banche dati del proprio studio professionale sia strutturata in modo idoneo e permetta anche di poter garantire agli interessati i diritti riconosciuti agli stessi dal GDPR, etc.).

In particolare, occorre considerare che gli Studi professionali detengono e gestiscono un ingente volume di informazioni di natura personale relativa non solo ai clienti, ma anche a collaboratori e dipendenti. Ciò rende queste realtà, piccoli o grandi che siano, un potenziale obiettivo dei cybercriminali. Una violazione della sicurezza dei dati può avere degli effetti legali, economici e reputazionali devastanti sia per i clienti, sia per gli stessi studi professionali. Per questo è fondamentale che i titolari del trattamento si dotino di misure di sicurezza efficaci, al fine di preservare la riservatezza, l'integrità e la disponibilità dei dati, specie di quelli appartenenti a categorie particolari (ai sensi dell'art. 10 del GDPR).

È stato osservato che spesso gli studi professionali sono oggetto di cyberattacchi a causa della mancanza di consapevolezza dei rischi da parte dei professionisti o della scarsità di risorse finanziarie adeguate a garantire misure tecnologiche efficaci contro attacchi ai sistemi informativi.
È il caso della violazione di un account di posta attraverso la tecnica del *phishing*, a cui può seguire la distribuzione di un ransomware (un virus in grado di criptare l'intero hard disk, impedendone l'accesso all'utilizzatore fino al pagamento di un riscatto, in genere in bitcoin) alle caselle di posta di altri professionisti, sfruttando il meccanismo di fiducia generato da e-mail inoltrate da Colleghi.
È importante, infine, sottolineare la necessità di un dialogo fra professionisti ed esperti in materia di nuove tecnologie e tutela dei dati personali a garanzia dei propri clienti, proprio come già avviene, ad esempio, allorché un ingegnere edile necessiti delle competenze specialistiche di un geologo per comprendere la composizione di un terreno e la sua idoneità ad accogliere una struttura sulla sua superficie, assolvendo, fra l'altro, a un preciso dovere deontologico.
Sulla base di quanto detto nelle premesse, si darà conto, di seguito, di alcune regole da seguire come buona prassi per impostare una corretta gestione degli strumenti informatici utilizzati nello svolgimento dell'attività lavorativa.

Perché è necessario trattare i dati personali?

In una società fortemente interconnessa come la nostra è impossibile prescindere dalla circolazione e dal trattamento dei dati personali: imprese, pubbliche amministrazioni, professionisti non potrebbero svolgere la loro attività senza la disponibilità dei dati personali dei clienti, dei cittadini o dei loro dipendenti/collaboratori.

Come recita il considerando 4 del GDPR, "il trattamento dei dati personali dovrebbe essere al servizio dell'uomo". Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali. Anche in tale prospettiva devono interpretarsi le condizioni di liceità del trattamento, di cui all'art. 5 del GDPR.

Il trattamento di dati personali, in effetti, può essere necessario per dare esecuzione a un contratto (o a misure precontrattuali) di cui l'interessato è parte (come l'espletamento di un incarico professionale affidato a un professionista), per ottemperare a un obbligo legale al quale il titolare del trattamento è soggetto (ad esempio, l'obbligo di conservazione decennale delle fatture contenenti dati riferiti a persone fisiche[1]), oppure può essere necessario per salvaguardare degli interessi vitali, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, oppure ancora – qualora non sia ravvisabile una delle citate condizioni per le quali sia necessario effettuare il trattamento - lo stesso è lecito qualora sia basato sul consenso o sul legittimo interesse del titolare o di terzi (a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato).

Il trattamento di dati personali, quindi, risulta un elemento imprescindibile della nostra società e della nostra economia, specie quella digitale, che deve essere regolamentato per favorirne la libera circolazione, ma al contempo garantire un livello elevato di protezione delle persone fisiche, alle quali è riconosciuto un diritto fondamentale[2] che non è assoluto, ma andrà di volta in volta andrà contemperato con gli altri diritti fondamentali, nel rispetto del principio di proporzionalità.

[1] Il GDPR infatti si riferisce solo ai dati di persone fisiche, come specificato più avanti.

[2] Si vedano gli artt. 8, par. 1, Carta dei diritti fondamentali dell'Unione europea e 16, par. 1, Trattato sul funzionamento dell'Unione europea, i quali stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

Nel linguaggio comune si fa spesso riferimento al termine "privacy" per indicare la tutela dei dati personali. In realtà, per privacy si intende il diritto alla riservatezza delle informazioni personali (non necessariamente dati personali) e della propria vita privata. La protezione dei dati personali se da un lato garantisce la riservatezza dei propri dati personali, dall'altra mira a consentire la libera circolazione degli stessi, purché siano trattati nel rispetto di principi e dei diritti degli interessati.

Che cos'è un dato personale?

Ogni informazione che faccia riferimento a una persona fisica identificata o soltanto identificabile è considerata un dato personale. La persona fisica, infatti, può essere identificata sia direttamente (ad esempio attraverso il nome e il cognome), sia indirettamente mediante l'utilizzo di più informazioni.

In sintesi, dunque, i dati personali che dobbiamo proteggere sono tutte le informazioni riferibili a una persona e che sono idonee a identificarla, anche in modo indiretto: non solo quindi il nome, il cognome e il codice fiscale, ma anche username e password per l'accesso alla posta elettronica, il codice di autenticazione al pc o al sistema informatico. Costituiscono un dato personale, infatti, tutte le informazioni che si riferiscono a una persona, come uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale[3].

L'indirizzo IP, ossia l'indirizzo assegnato dal provider di servizi internet al dispositivo collegato alla rete (PC, smartphone, tablet, stampante, etc.), è considerato un dato personale, dal momento che il fornitore del servizio di rete dispone di ulteriori informazioni (ora di accesso, siti visitati, etc.) che associati all'indirizzo IP gli consente di identificare una persona fisica.

[3] Cfr. art. 4, n. 1), GDPR. È 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";

Che cosa sono i dati personali appartenenti a categorie particolari?

I dati personali appartenenti a categorie particolari[4] sono informazioni relative a una persona fisica identificata o identificabile, idonee a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale; sono, altresì, dati personali appartenenti a categorie particolari i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale.

I dati personali appartenenti a categorie particolari devono essere protetti con attenzione, secondo il principio dell'accountability[5], poiché il loro trattamento espone a molteplici rischi i diritti e le libertà degli interessati.

Cosa si intende per trattamento?

In generale, un trattamento di dati personali è qualsiasi operazione applicata a dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, la modica, l'uso, la consultazione, la comunicazione, la trasmissione, ma anche la distruzione dei dati, effettuata con qualsiasi mezzo, indipendentemente se cartaceo, elettronico, digitale, posta in essere manualmente o tramite procedure informatiche automatizzate. Ad esempio, registrare e organizzare dati personali all'interno di un database, leggerli, consultarli come pure cancellarli è un trattamento[6].

A chi appartengono i dati personali? – l'interessato

L'interessato è colui al quale appartengono i dati personali ed è sempre una persona fisica e mai una persona giuridica, identificata o identificabile[7].

I dati personali trattati durante l'attività professionale non appartengono al professionista che li ha raccolti o li tratta, poiché quest'ultimo non è libero di trattarli senza seguire le regole imposte

[4] Cfr. art. 9 GDPR.
[5] In relazione al quale si vedano i paragrafi seguenti.
[6] Cfr. art. 4, n. 2), GDPR. Per trattamento si intende "*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*".
[7] Cfr. art. 4, n. 1), GDPR.

dal GDPR, dal Codice in materia di protezione dei dati personali e dai provvedimenti rilevanti in materia emanati dall'Autorità Garante. È per questo, ad esempio, che l'interessato ha il diritto di essere informato sulle finalità e i mezzi del trattamento, ricevendo idonea informativa, nonché di esercitare i diritti di cui agli artt. 15-22 del GDPR, tra cui quello di chiedere l'accesso ai propri dati personali o la loro cancellazione[8] al titolare del trattamento, ossia - nel caso specifico – al professionista che li tratta in esecuzione di un incarico professionale.

[8] Sui diritti degli interessati, si veda il paragrafo "Predisporre le procedure per garantire l'esercizio dei diritti degli interessati".

Perché il professionista deve trattare correttamente i dati personali?

Il professionista – o lo studio professionale - è tenuto a trattare correttamente i dati personali gestiti in esecuzione di un incarico professionale in quanto, determinando in relazione agli stessi le finalità e i mezzi del trattamento, risulta esserne il titolare[9].

Il titolare del trattamento[10] è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali. Può quindi essere il professionista o la società costituita da più professionisti che determina le finalità del trattamento (fornire l'attività di consulenza, contattare e/o rispondere alle richieste del cliente, etc.) nonché i mezzi del trattamento stesso (servendosi di strumenti cartacei e/o informatici, etc.).

In particolare, il professionista – o lo studio professionale -, in quanto titolare del trattamento, deve mettere in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR (art. 24, par. 1), quindi a trattare i dati in modo lecito, corretto e trasparente nei confronti dell'interessato (art. 5 GDPR). Perché il titolare del trattamento deve fare tutto questo? Il GPDR non deve essere visto come un libretto di istruzioni puntuali, da seguire pedissequamente, quanto, piuttosto, come un insieme di coordinate che servono a guidare il titolare del trattamento nelle attività che comportano una gestione dei dati personali, lasciando che sia lo stesso titolare a prevedere e implementare le misure tecniche e organizzative che ritiene, sulla base delle verifiche effettuate, più efficaci a tutelare i diritti e le libertà degli interessati. In questo modo, il titolare si assume la responsabilità delle misure adottate: è il c.d. **principio di accountability** previsto all'art. 5, p. 2, GDPR, che impone al titolare del trattamento non solo, come si è detto, di adottare misure idonee a proteggere i dati personali trattati, ma anche di essere in grado di provarle e vedremo nel prosieguo in che modo.

I professionisti e i loro collaboratori/dipendenti trattano quotidianamente diversi tipi di dati personali, appuntando i dati anagrafici di un cliente su un foglio di carta o inserendoli in un

[9] Si veda art. 4, par. 1, n. 7), GDPR. Come anche specificato Dall'European Data Protection Board nelle "Guidelines 07/2020 on the concepts of controller and processor in the GDPR", il titolare è colui che decide gli elementi chiave del trattamento.

database, inviando una e-mail, cancellando un numero di telefono dalla rubrica dello studio professionale, etc.

Il trattamento di questi dati passa, come vedremo, attraverso una serie di attività che il professionista o lo studio professionale (titolare del trattamento) deve compiere per garantire la correttezza e la liceità del trattamento.

Il trattamento dei dati personali nel rispetto delle disposizioni previste dalla legge permette, inoltre, di:

- garantire l'efficienza dell'attività professionale. I dati personali correttamente trattati, infatti, assicurano un ordinato svolgimento delle prestazioni professionali, ottimizzando tempi e procedure;
- fidelizzare i propri clienti e acquisirne di nuovi, rafforzando il *personal branding*;
- evitare di esporsi ai provvedimenti sanzionatori da parte delle autorità competenti e/o alle azioni risarcitorie dei clienti[11].

[11] Sulle conseguenze sanzionatorie in caso di violazione delle disposizioni del GDPR, si veda più avanti.

Come assicurare il corretto trattamento dei dati personali

Come accennato in precedenza, il professionista titolare del trattamento deve compiere una serie di attività finalizzate a garantire la correttezza e la liceità del trattamento stesso:

1. effettuare delle verifiche preliminari e mappare i trattamenti;
2. predisporre il registro dei trattamenti;
3. individuare ruoli e responsabilità all'interno dello studio professionale;
4. redigere l'informativa sul trattamento dei dati personali;
5. analizzare i rischi e definire le misure di sicurezza necessarie a limitare tali rischi;
6. predisporre precise procedure per garantire l'esercizio dei diritti degli interessati[12].

[12] I temi qui riportati in elenco sono sviluppati nei paragrafi successivi.

La mappatura dei trattamenti

Si tratta di un'operazione fondamentale volta a individuare i trattamenti effettuati all'interno dello studio professionale, i tipi di dati personali trattati, con quali strumenti avviene il trattamento di tali dati e quali sono i soggetti coinvolti nel trattamento.
In particolare, il titolare del trattamento dovrà:

- mappare gli strumenti e le risorse informatiche interne, ad esempio:
  - i gestionali utilizzati (negli studi professionali maggiormente strutturati)
  - i sistemi operativi utilizzati, che spesso presentano differenti vulnerabilità
  - gli applicativi utilizzati
  - gli account di posta elettronica e di posta elettronica certificata (PEC)

- mappare eventuali trattamenti elettronici particolari, quali ad esempio:
  - presenza di un sistema di videosorveglianza
  - presenza di dispostivi o risorse informatiche a uso promiscuo (smartphone, tablet, etc. utilizzati da più professionisti o collaboratori/dipendenti)

- mappare le banche dati elettroniche e/o cartacee (archivio documenti dipendenti, database clienti, elenco fornitori, cartelle di documenti relativi alla fatturazione elettronica, archivio pratiche e progetti, etc.)

- mappare gli strumenti e le risorse fisiche interne quali ad esempio:
  - presenza di un sistema di allarme
  - presenza di aree o contenitori ad accesso selezionato e gestione delle relative chiavi
  - presenza di strumenti distruggi documenti
  - gestione di dorsi di raccoglitori, intestazione di fascicoli, etc.

Il registro delle attività di trattamento

La mappatura dei trattamenti avviene mediante l'ausilio del registro delle attività di trattamento, disciplinato dall'art. 30 del GDPR, strumento indispensabile di cui il professionista, in qualità di titolare, è obbligato a dotarsi, trattando i dati personali in maniera non occasionale[13].

Il registro delle attività di trattamento, in realtà, oltre ad essere un documento la cui adozione è obbligatoria, può rivelarsi uno "strumento" molto utile, non solo per monitorare le tipologie e le caratteristiche delle attività di trattamento, ma anche sotto il profilo della gestione e del controllo delle dinamiche e dei flussi di informazioni che caratterizzano le attività dello studio professionale, nonché dei soggetti che – a vario titolo - intervengono nel trattamento dei dati di cui lo studio professionale è titolare. Proprio per questo, al di là degli elementi obbligatori, il registro dei trattamenti è tanto più utile al professionista quanto più risulta essere accuratamente predisposto e tempestivamente aggiornato ad ogni modifica che abbia un impatto sui trattamenti di dati personali.

Il registro deve contenere:

a) il nome e i dati di contatto del titolare del trattamento e, se sono presenti, del contitolare del trattamento[14], del rappresentante del titolare del trattamento e del responsabile della protezione dei dati.

Il rappresentante del titolare o del responsabile del trattamento è la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del GDPR. Si, tratta, quindi di una figura che andrà nominata solo se lo studio professionale o il professionista non è stabilito in un paese dell'Unione Europea.

Il responsabile della protezione dei dati, meglio conosciuto come **DPO** (Data Protection Officer), è una figura obbligatoria ove ricorra una delle condizioni previste dall'art. 37 del GDPR[15]. Negli altri casi, la nomina del DPO – seppur non obbligatoria - è ovviamente possibile,

[13] Cfr. art. 30, GDPR.
[14] Per una definizione di contitolare si veda più avanti il paragrafo "Redigere la documentazione necessaria".
[15] Ai sensi dell'art. 37, p. 1, "*Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:*

come opzione organizzativa ulteriore e di maggior cautela ed è, anzi, fortemente raccomandata dal Garante per la protezione dei dati personali.

Rientrano tra i compiti del DPO:

- informare e consigliare il titolare o il responsabile, e i loro dipendenti;
- assicurare il rispetto del regolamento e della legge nazionale in merito alla protezione dei dati;
- informare l'organizzazione sulla realizzazione di studi di impatto sulla protezione dati e verificarne l'esecuzione;
- collaborare con il Garante ed esserne il punto di contatto.
- collaborare nell'adeguamento agli obblighi imposti dal regolamento europeo, fornendo informazioni sul contenuto dei nuovi obblighi imposti dal regolamento europeo;
- condurre un inventario del trattamento dei dati della propria organizzazione;
- progettare azioni di sensibilizzazione;
- gestire in maniera continuativa la conformità dell'organizzazione al regolamento.

Le responsabilità che sorgono in capo alla persona designata come DPO sono quindi rilevantissime e richiedono competenze trasversali, sia legali che tecniche.

La figura del DPO è obbligatoria, oltre che per gli enti pubblici, anche per quei titolari che effettuano trattamenti su larga scala, che mirano, cioè, a trattare una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati.

Il singolo professionista che, in forma individuale, tratta solo i dati dei propri clienti generalmente non è tenuto alla designazione di un DPO[16].

---

a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure
c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10".

[16] Cfr. Cons. 91, GDPR e "Linee guida sui responsabili della protezione dei dati (RPD)" del Gruppo WP29, del 13 dicembre 2016.

b) le finalità del trattamento;

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

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

e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

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

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

Il registro deve contenere tutti gli elementi di cui all'art. 30, par. 1, GDPR[17] e deve essere tenuto costantemente aggiornato, in quanto il suo contenuto deve sempre corrispondere ai trattamenti effettivamente posti in essere.

Per redigere il registro, sarà sufficiente predisporre un foglio in formato excel, come mostrato sinteticamente di seguito.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

SCHEDA REGISTRO DEI TRATTAMENTI *[per i contenuti vedi Faq sul registro delle attività di trattamento: https://www.garanteprivacy.it/regolamentoue/registro]*							
TITOLARE/CONTITOLARE/RAPPRESENTANTE DEL TITOLARE *[inserire la denominazione e i dati di contatto]*							
RESPONSABILE DELLA PROTEZIONE DEI DATI *[inserire la denominazione e i dati di contatto]*							
TIPOLOGIA DI TRATTAMENTO	FINALITA' E BASI LEGALI DEL TRATTAMENTO	CATEGORIE DI INTERESSATI	CATEGORIE DI DATI PERSONALI	CATEGORIE DI DESTINATARI *[indicare eventuali responsabili del trattamento o altri titolari cui i dati siano comunicati]*	TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI *[indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le "garanzie" adottate ai sensi del capo V del RGPD]*	TERMINI ULTIMI DI CANCELLAZIONE PREVISTI	MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

Tabella 1: Modello di "registro semplificato" delle attività di trattamento del titolare, Autorità Garante per la protezione dei dati personali

[17] Secondo l'art. 30, par. 2, il registro deve essere tenuto oltre che in qualità di titolare, anche come eventuale responsabile del trattamento. Per un approfondimento sul responsabile del trattamento, si vedano i paragrafi successivi.

Individuare ruoli e responsabilità all'interno dello studio professionale

Contestualmente alla redazione del registro dei trattamenti, nella sua qualità di titolare del trattamento, il professionista deve interrogarsi sul ruolo svolto dai soggetti che fanno parte dello studio professionale, individuando le figure previste dal GDPR e le relative responsabilità.

Sono **soggetti attivi** del trattamento:

a) il titolare del trattamento e gli eventuali contitolari;

b) il responsabile del trattamento;

c) il rappresentante del titolare o del responsabile del trattamento;

d) i collaboratori/dipendenti autorizzati o designati dal titolare.

Soggetto passivo del trattamento è l'interessato.

Il titolare del trattamento

Il titolare del trattamento è stato già definito come la persona fisica o giuridica che fissa le finalità e i mezzi del trattamento[18].

Il professionista, in qualità di titolare del trattamento, deve:

1) rispettare i principi applicabili al trattamento dei dati personali previsti dall'art. 5[19];

2) rispettare i principi di privacy by design e privacy by default, previsti dall'art. 25, GDPR;

3) mettere in atto misure tecniche e organizzative adeguate a garantire trattamenti conformi al Regolamento[20];

4) tenere il registro delle attività di trattamento ove obbligatorio o comunque opportuno[21];

5) adottare una adeguata procedura di data breach[22];

[18] Si vedano i paragrafi precedenti.
[19] Si vedano i paragrafi successivi.
[20] Si veda il paragrafo "Sicurezza dei dati personali".
[21] V. sopra.
[22] V. più avanti.

6) effettuare la valutazione d'impatto sulla protezione dei dati (PIA) ed effettuare eventualmente una consultazione preventiva avanti all'Authority[23];

7) stipulare un accordo con eventuali contitolari del trattamento per disciplinare le rispettive responsabilità;

8) disciplinare il rapporto con il responsabile del trattamento mediante un contratto o altro atto giuridico oppure clausole contrattuali tipo;

9) istruire chiunque agisca sotto la propria autorità[24].

Contitolarità

Può capitare che le finalità e i mezzi del trattamento siano determinati congiuntamente da più soggetti. Si parla in questo caso di **contitolarità**, prevista dall'art. 26, GDPR, ad esempio nella gestione comune di clientela all'interno dello stesso studio professionale.

I contitolari devono redigere un accordo in cui, in maniera trasparente, precisano:

a) le rispettive responsabilità quanto al rispetto degli obblighi derivanti dal GDPR e, in particolare, le modalità di esercizio dei diritti da parte dell'interessato e le modalità con cui comunicare le informazioni previste dagli articoli 13 e 14, GDPR[25];

b) i rispettivi ruoli e rapporti con l'interessato.

L'accordo, nei suoi punti essenziali, deve essere messo a diposizione dell'interessato, che può, comunque, esercitare i propri diritti verso l'uno o l'altro contitolare.

Accertare la contitolarità presuppone sempre una valutazione in concreto, verificando se le finalità e i mezzi del trattamento siano o meno determinati congiuntamente. Casi apparenti di contitolarità, infatti, potrebbero rientrare nella titolarità autonoma dei professionisti.

Due Professionisti ricevono un incarico dallo stesso committente per la realizzazione di un'opera. Il primo si occuperà della fase progettuale, il secondo della direzione dei lavori, trattando i dati personali attraverso i propri dispositivi e servendosi dei propri collaboratori/dipendenti. In tal caso le finalità e i mezzi del trattamento sono determinati

[23] Si veda più avanti.
[24] Cfr. art. 29, GDPR e art. 2-quaterdecies, D.Lgs. 196/2003 (Codice Privacy).
[25] Su cui v. più avanti.

autonomamente da ciascun professionista, che resterà titolare autonomo del trattamento dei dati personali raccolti.

Il responsabile del trattamento

Il responsabile del trattamento è quel soggetto, esterno all'organizzazione del professionista o dello studio professionale titolare del trattamento, che tratta dati personali per conto di quest'ultimo[26] (e che, quindi, non determina le finalità e i mezzi del trattamento stesso[27]).

Sono, quindi, responsabili del trattamento tutti quei soggetti esterni ai quali il professionista affida l'esecuzione di alcuni trattamenti di dati personali, come ad esempio i fornitori di servizi informatici[28], che possono avere accesso ai dati personali trattati dal professionista.

Prima di affidare il trattamento ad un responsabile, il titolare deve stipulare un contratto o accordo scritto (anche in formato elettronico) che specifichi[29]:

a) la durata del trattamento;

[26] "Il responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento" (art. 4, n. 8), GDPR).

[27] Salvo i casi di mezzi "non essenziali", come meglio specificato nelle citate EDPB 7/2020 "Guidelines on the concepts of controller and processor in the GDPR".

[28] Sulla qualifica dei soggetti che svolgono servizi informatici per conto del titolare si vedano gli esempi riportati al paragrafo 81 delle menzionate Guidelines EDPB 7/2020.

[29] Cfr. art. 28, GDPR. In particolare, il paragrafo 3, lett. a) - h), prevede che il contratto o accordo debba specificare che il responsabile del trattamento:

"a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

c) adotti tutte le misure richieste ai sensi dell'articolo 32;

d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;

e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, 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;

f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e

h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato".

b) la natura e le finalità del trattamento (ad esempio, per eseguire la manutenzione dei dispositivi e/o dei sistemi informatici utilizzati dal professionista);
c) il tipo di dati personali e le categorie di interessati (ad esempio, collaboratori/dipendenti, clienti, etc.);
d) gli obblighi e i diritti del titolare.

Il consulente del lavoro è un responsabile del trattamento?

- I consulenti del lavoro sono titolari del trattamento quando trattano, in piena autonomia e indipendenza, i dati dei propri dipendenti oppure dei propri clienti quando siano persone fisiche, come ad esempio i **liberi professionisti**, determinando puntualmente le finalità e i mezzi del trattamento;
- Sono, viceversa, responsabili quando trattano i dati dei dipendenti dei loro clienti sulla base dell'incarico ricevuto, che contiene anche le istruzioni sui trattamenti da effettuare. È il caso, ad esempio, dei consulenti che curano per conto di datori di lavoro la predisposizione delle buste paga, le pratiche relative all'assunzione e al fine rapporto, o quelle previdenziali e assistenziali, trattando una pluralità di dati personali, anche appartenenti a categorie particolari, dei lavoratori[30].

Chi risponde dei danni subiti dall'interessato per violazione delle disposizioni del GDPR?

In linea generale è prima di tutto il titolare che risponde per il danno cagionato dal suo trattamento, anche quando a sbagliare è stato il responsabile, perché sul titolare incombe un obbligo non solo di corretta selezione del responsabile del trattamento (c.d. *culpa in eligendo*), ma anche di puntuale controllo dell'attività svolta dallo stesso responsabile (c.d. *culpa in vigilando*). Il titolare è, quindi, esonerato dalla responsabilità solo se prova che il danno non dipende in alcun modo da un suo comportamento.

Tale principio, in realtà, è stato "ammorbidito" dal GDPR che prevede, favorendo la parte debole del trattamento (l'interessato), che il titolare e il responsabile del trattamento siano responsabili in solido per l'intero ammontare del danno e, pertanto, l'interessato possa chiedere

[30] Per ulteriori approfondimenti si veda l'esempio riportato al paragrafo 38 ("Payroll administration") delle citate Guidelines EDPB 7/2020.

il risarcimento del danno sia al titolare che al responsabile[31]. Tuttavia, qualora un titolare del trattamento o un responsabile del trattamento abbia pagato l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno.

Gli amministratori di sistema (AdS)

I fornitori di servizi informatici, oltre a rivestire il ruolo di responsabile del trattamento, possono trovarsi a esercitare anche le funzioni di **amministratore di sistema** (AdS), che comportano l'adempimento di ulteriori formalità.

L'AdS non è espressamente previsto dal GDPR, ma è definito dal Provvedimento del Garante per la protezione dei dati personali (GPDP) del 27 novembre del 2008 come "*una figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise resource planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali*".

In presenza di un AdS e seguendo le prescrizioni del GPDP, il professionista che affida il servizio di gestione e manutenzione a un soggetto esterno (responsabile del trattamento) dovrà:

a) designare tale soggetto amministratore di sistema, a mezzo di un atto che deve elencare analiticamente gli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;

b) adottare idonei sistemi di controllo che consentano la registrazione degli accessi logici da parte degli amministratori ai sistemi di elaborazione e agli archivi elettronici. L'accesso di ciascun amministratore (access log), quindi, deve essere registrato e conservato per almeno 6 mesi, con caratteristiche di completezza, integrità ed inalterabilità e deve comprendere anche i riferimenti temporali, la descrizione dell'evento e del sistema coinvolto;

c) verificare l'operato degli AdS con cadenza almeno annuale, per accertare che le attività svolte dall'amministratore siano effettivamente conformi alle mansioni attribuite;

[31] Cfr. art. 82, GDPR.

d) conservare l'elenco con i nominativi degli AdS. Tale adempimento può essere affidato allo stesso responsabile del trattamento.

Chi è l'amministratore di sistema quando il responsabile del trattamento è una società?

Quando a trattare i dati per conto del titolare è una società o comunque un'organizzazione, intesa come un'entità diversa dalla persona fisica, la qualità di responsabile è rivestita dalla società o dall'organizzazione e non dalla persona fisica che ne ha il potere di rappresentanza sul piano giuridico. Se, poi, all'interno della società o dell'organizzazione del responsabile del trattamento ci siano una o più persone fisiche che svolgono anche il ruolo di amministratore di sistema, spetterà alla società o all'organizzazione responsabile del trattamento impartire ai propri dipendenti/collaboratori che svolgono tale delicato ruolo le relative istruzioni per svolgere correttamente e in linea con il GDPR le mansioni di AdS. I nominativi delle persone fisiche che svolgono il ruolo di AdS dovranno a richiesta essere messi a disposizione del titolare del trattamento.

Gli autorizzati al trattamento

I dipendenti e/o i collaboratori dello studio professionale, in qualità di autorizzati al trattamento, dovranno ricevere dal titolare adeguate istruzioni sui trattamenti di dati personali da svolgere sotto l'autorità dello stesso[32]. Il titolare, inoltre, si assume la responsabilità in caso di violazioni delle disposizioni in materia di protezione dei dati personali da parte degli autorizzati.
Risulta fondamentale, quindi, la corretta e puntuale formazione dei collaboratori/dipendenti e l'adozione di una policy chiara e dettagliata che metta gli autorizzati nella condizione di adempiere correttamente alle norme previste dalla normativa sulla protezione dei dati personali, garantendo i diritti e le libertà degli interessati.

[32] Cfr. art. 29 GDPR.

I principi applicabili al trattamento dei dati personali

Liceità, correttezza e trasparenza.

Ogni trattamento dei dati personali deve essere lecito e corretto. Le modalità con cui i professionisti raccolgono, utilizzano, consultano i dati personali devono essere rese note agli interessati. Lo strumento attraverso cui si attua il principio della trasparenza è rappresentato dall'informativa, nella quale il professionista, con un linguaggio semplice e chiaro, illustra le informazioni e le comunicazioni relative al trattamento di tali dati e in particolare:

- l'identità del titolare del trattamento;
- i dati di contatto del responsabile della protezione dei dati (RPD o DPO), laddove presente;
- finalità e base giuridica del trattamento;
- il periodo di conservazione dei dati personali o comunque i criteri utilizzati per determinare tale periodo;
- i diritti riconosciuti all'interessato, fra i quali quello di accesso, rettifica, cancellazione, limitazione e il diritto di opporsi al loro trattamento.

Limitazione delle finalità del trattamento

L'utilizzo dei dati personali è limitato agli obiettivi fissati per la realizzazione dei servizi professionali pattuiti.

Il professionista non potrà trattare i dati raccolti attraverso una visura catastale per finalità diverse da quelle relative all'espletamento dell'incarico professionale conferito dal cliente e in virtù del quale acquisisce i dati personali relativi alla visura catastale.

Minimizzazione dei dati

Definire le finalità del trattamento permette di stabilire se i dati personali raccolti siano adeguati, pertinenti e necessari alle finalità stesse.
Una raccolta di dati eccessiva sul piano quantitativo o sul piano qualitativo (non pertinente alle finalità fissate), viola il principio di minimizzazione.

Esattezza dei dati

È importante che i dati personali siano costantemente aggiornati e, se necessario, cancellati una volta esaurite le finalità per le quali sono stati trattati. Tale principio è correlato ai diritti di rettifica e cancellazione riconosciuti dagli articoli 16 e 17 del GDPR agli interessati.

Il cambio dell'indirizzo di residenza, del domicilio, del numero di telefono, etc., se comunicati dal cliente, impongono un aggiornamento dei dati personali riferibili all'interessato.

Durata limitata del trattamento

Il trattamento dei dati personali da parte del professionista non può protrarsi oltre il tempo necessario per l'espletamento degli incarichi, ovvero oltre il tempo necessario in funzione del mandato e della finalità del trattamento stesso, compresi gli obblighi legali di conservazione; nell'informativa al cliente è essenziale indicare il periodo di trattamento, compresa la conservazione dei dati personali o i criteri utilizzati per determinare tale periodo.

Ad esempio, nell'informativa resa al cliente (interessato al trattamento), il professionista dovrà indicare il periodo di trattamento di dati personali, in relazione al criterio del tempo necessario all'espletamento dell'incarico affidato, e in particolare anche il periodo di conservazione dei dati personali, sulla scorta degli obblighi di legge o delle norme professionali che impongono al professionista la successiva conservazione del fascicolo contenente dati personali (a prescindere dal fatto che si tratti di fascicolo informatico o cartaceo).

Integrità e Riservatezza[33]

Il professionista è tenuto, anche per obblighi deontologici e nel rispetto del segreto professionale, ad approntare un adeguato livello di sicurezza per i dati dei clienti. Egli, pertanto, nella sua qualità di titolare del trattamento deve prevedere tutte le misure necessarie per garantire la confidenzialità, integrità e disponibilità dei dati personali.

I dati contenuti nel fascicolo, ad esempio, non possono essere consultati da persone non abilitate ed espressamente autorizzate e istruite ad accedervi in ragione dei loro specifici compiti, sia che si tratti di soggetti interni all'organizzazione dello studio professionale (addetti alla segreteria, praticanti, colleghi di studio) o esterni allo stesso (altri professionisti che collaborano al medesimo progetto, consulenti tecnici, commercialisti, etc.).

Privacy by design e privacy by default[34]

Il professionista è chiamato a implementare tutte le misure di sicurezza tecniche e organizzative necessarie ad assicurare il rispetto dei principi appena elencati e dei diritti e delle libertà degli interessati (essendo, altresì, in grado di dimostrarlo), prima di iniziare un trattamento di dati personali (by design) e preferire tutte quelle soluzioni (in particolare software) le cui impostazioni garantiscano già (by default) il rispetto di quei principi e di quei diritti e libertà.

---

[33] Per una disamina più approfondita delle misure tecniche e organizzative da approntare si veda il paragrafo "Sicurezza dei dati personali".

[34] 1. Ai sensi dell'art. 25, par. 1 e 2, GDPR, "*Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.*

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

I principi di privacy by design e by default sono fra loro complementari, nel senso che l'uno garantisce il rispetto dell'altro e, pertanto, vanno sempre considerati unitariamente.

Per **privacy by design** si intendono tutte quelle misure tecniche e organizzative che il titolare del trattamento è tenuto a adottare, a pensare, prima di iniziare un trattamento dei dati personali, al fine di garantire l'effettività dei principi di cui al n. 1) e dei diritti e libertà degli interessati.

Non esistono misure tecniche e organizzative uguali per tutti. il professionista dovrà:

a) tenere conto della specificità della propria attività e adattare, di volta in volta, le misure tecniche e organizzative al livello di rischio che il trattamento rappresenta per i diritti e le libertà degli interessati;

b) documentare le sue scelte (nel registro dei trattamenti) in modo da essere in grado di provare di aver adottate misure adeguate (accountability).

Inoltre, nel prevedere tali misure il professionista tiene conto:

a) dello **"stato dell'arte"**, cioè qual è il livello tecnologico raggiunto e quali misure, quindi, possano garantire la miglior tutela disponibile per i diritti e le libertà degli interessati.

b) dei costi di attuazione. Se una misura è la più evoluta, tenendo conto lo stato dell'arte, ma eccessivamente onerosa per il professionista, potrà essere scartata, documentando la scelta di adottare misure meno costose, ma comunque idonee a garantire i diritti e le libertà degli interessati.

c) della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento. Come detto non esistono misure tecniche e organizzative standard, uguali per tutti;

d) dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento.

Il principio di privacy by design non si riferisce soltanto alle misure tecniche, ma anche a quelle organizzative: l'assenza di misure organizzative efficaci può vanificare l'efficacia delle misure tecniche adottate. Per questo, come si vedrà, è importante rimanere aggiornati sull'uso delle tecnologie e sulle regole in materia di protezione dei dati e prevedere un piano di aggiornamento per i collaboratori/dipendenti.

Il principio di **privacy by default** impone al titolare del trattamento di prevedere che le configurazioni del sistema di trattamento dei dati personali utilizzato (un gestionale, un dispositivo portatile, etc.) limitino quanto più possibile il numero di dati trattati, la durata del trattamento, il periodo di conservazione dei dati e la loro accessibilità.

Questo significa che, per impostazione predefinita, il professionista non dovrebbe raccogliere più dati di quanto non sia necessario per le finalità previste, né conservarli per un periodo indefinito. Per questo, nella scelta di un software per la gestione dei clienti, ma anche nella predisposizione di misure organizzative (ad esempio il numero dei collaboratori/dipendenti ad accedere a certe categorie di dati personali dei clienti), il professionista dovrebbe preferire quelle soluzioni che già prevedono, appunto di default, un trattamento dei dati personali limitato a quanto strettamente necessario per conseguire le finalità previste.

Il principio di privacy by default influenza anche le decisioni di acquisto. Un professionista decide di acquistare un software per la gestione della clientela e mette a confronto due soluzioni: la prima prevede di default la necessità di inserire fra i dati richiesti il sesso del cliente, senza possibilità di eliminare o saltare il relativo campo, non prevede il cambio di password decorso un certo periodo di tempo e non ha una funzione per la cifratura dei dati; la seconda, invece, pur prevedendo il campo relativo al sesso del cliente, consente di eliminarlo o ignorarlo, permette di cambiare automaticamente la password, decorso un certo periodo di tempo e ha una funzione di cifratura dei dati.
In virtù del principio di privacy by default, il professionista dovrebbe optare per l'acquisto della seconda soluzione.

Il principio di trasparenza: l'informativa sul trattamento dei dati personali

Contenuto dell'informativa

Ai sensi dell'art. 13 del GDPR, nel momento in cui il professionista (titolare del trattamento) raccoglie i dati personali è tenuto a fornire all'interessato le seguenti informazioni:

a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;

b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;

c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento (consenso, interesse legittimo, adempimento di un obbligo legale, etc.);

d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;

e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali (subappaltatori, altri professionisti, etc.);

f) l'eventuale trasferimento dei dati in un paese non appartenente all'Unione Europea.

Sono previste, poi, ulteriori informazioni che il professionista deve fornire all'interessato al momento della raccolta dei dati personali:

a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati[35];

c) qualora il trattamento sia basato sul consenso[36], l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;

[35] Cfr. artt. 15 – 22, GDPR.
[36] Art. 6, par. 1, lett. a oppure art. 9, par. 2, lett. a), GDPR.

d) il diritto di proporre reclamo a un'autorità di controllo;

e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;

f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Se il professionista intende trattare i dati personali già acquisiti per una diversa finalità, sarà necessario rendere le pertinenti informazioni all'interessato.

Non vi è obbligo di fornire le informazioni di cui all'art. 13, GDPR, qualora queste siano già in possesso dell'interessato.

...se i dati non sono stati raccolti presso l'interessato?

Nell'adempimento del mandato può accadere che il professionista raccolga dati personali dal cliente che appartengono, però, a terzi interessati non presenti in quel momento.

L'art. 14, GDPR prevede in questo caso che l'informativa sia fornita all'interessato entro un termine ragionevole che non può superare un mese dalla raccolta, oppure:

- al più tardi al momento della prima comunicazione all'interessato, nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato;
- non oltre la prima comunicazione dei dati personali, nel caso in cui sia prevista la comunicazione ad altro destinatario.

Le informazioni non dovranno essere comunicate all'interessato se:

a) l'interessato dispone già delle informazioni;

b) comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato[37];

[37] In particolare, per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1, o nella misura in cui l'obbligo di cui al paragrafo 1 del presente articolo rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni.

c) l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato; oppure
d) qualora i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri, compreso un obbligo di segretezza previsto per legge[38].

Come va resa l'informativa?

Seguendo le indicazioni fornite dal Garante per la protezione dei dati personali e quelle contenute nel considerando n. 58, l'informativa dovrà essere concisa, trasparente, intelligibile per l'interessato e facilmente accessibile; occorre utilizzare un linguaggio chiaro e semplice, e per i minori occorre prevedere informative idonee[39].

L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico (soprattutto se resa dal professionista attraverso il proprio sito web), anche se sono ammessi "altri mezzi", quindi può essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui all'art. 12, paragrafo 1, GDPR. Il regolamento ammette, soprattutto, l'utilizzo di icone per presentare i contenuti dell'informativa in forma sintetica, ma solo "in combinazione" con l'informativa estesa; queste icone dovranno essere identiche in tutta l'Ue e saranno definite prossimamente dalla Commissione europea.

Le basi giuridiche del trattamento

Affinché il trattamento dei dati personali possa dirsi lecito è necessario che il titolare lo effettui in virtù di una o più delle basi giuridiche previste dall'art. 6, GDPR.

1) Il consenso dell'interessato

Attraverso il consenso l'interessato autorizza il titolare a trattare i propri dati personali per le finalità specifiche individuate nell'informativa.

[38] Quindi qualsiasi professionista deontologicamente tenuto al segreto professionale può avvalersi di tale esonero.
[39] Cfr. Considerando n. 58, GDPR.

Il consenso deve essere:

a) libero, cioè non condizionato: il mancato conferimento del consenso non può avere conseguenze negative per l'interessato[40];

b) inequivocabile. Il consenso deve essere espresso con un'azione positiva inequivocabile con cui l'interessato manifesta l'intenzione di accettare il trattamento. Occorre verificare che la richiesta di consenso sia chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato, per esempio all'interno della modulistica.

La casella presente sul sito web del professionista con cui si richiede all'utente di esprimere il proprio consenso all'invio di una newsletter, non può essere già spuntata.
Il modulo che reca l'informativa e la richiesta del consenso, non può presentare caselle già spuntate.

c) specifico, cioè relativo alla finalità per la quale è eseguito il trattamento. Se il trattamento ha diverse finalità, il consenso deve essere espresso per ciascuna finalità.

d) informato, quindi espresso dopo aver preso visione dell'informativa di cui all'art. 13, GDPR.

e) verificabile. Il titolare deve essere in grado di provare che l'interessato ha espresso il proprio consenso al trattamento dei dati e per quella o quelle specifiche finalità, ma non è obbligato a documentarlo per iscritto, anche se è consigliabile in ogni caso.

f) revocabile. L'interessato deve poter revocare il proprio consenso in ogni momento e con la stessa facilità con cui lo ha espresso.

2) Esecuzione di un contratto di cui l'interessato è parte

Quasi sempre il professionista può giustificare il proprio trattamento sulla base di un contratto stipulato con il cliente. Il consenso dell'interessato, infatti, non è necessario e non deve essere

[40] Cfr. art. 7, par. 4, GDPR "*Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto*".

richiesto quando il rapporto fra professionista e cliente si fonda su un contratto, che legittima il correlativo trattamento dei dati.

3) Adempimento di un obbligo legale al quale è soggetto il titolare del trattamento

Il professionista è tenuto a conservare le fatture e, quindi, a trattare i dati personali in esse contenuti per 10 anni dalla loro emissione

4) Interesse legittimo del titolare del trattamento

Il trattamento dei dati personali mediante un sistema di videosorveglianza è giustificato dall'interesse legittimo del professionista a tutelare i beni aziendali e l'incolumità propria e degli eventuali collaboratori/dipendenti

I diritti degli interessati

Il diritto di accesso ai dati[41]

L'interessato ha diritto di chiedere al titolare:

- se sta trattando i suoi dati personali;
- la comunicazione dei dati in forma comprensibile e tutte le informazioni disponibili per quanto attiene l'origine del trattamento;
- le informazioni sulla finalità del trattamento, i dati raccolti e i destinatari;
- il periodo di conservazione dei dati e, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'esistenza del diritto di chiedere la rettifica, la cancellazione, la limitazione dei dati personali o del diritto di opporsi al trattamento;
- il diritto di proporre reclamo a un'autorità di controllo (il Garante per la protezione dei dati personali).

Quali aspetti deve tenere in considerazione il titolare?

Tempo di risposta a una richiesta[42]:

a) senza ingiustificato ritardo e comunque entro 1 mese dalla richiesta;

b) entro un termine superiore a 1 mese dalla richiesta, tenuto conto della complessità e del numero di richieste, a condizione che l'interessato riceva comunque un'informazione al riguardo entro un mese dal ricevimento della richiesta.

Per disciplinare tali aspetti, è fondamentale che il titolare del trattamento adotti e applichi una precisa procedura per il riscontro dei diritti degli interessati.

A tal fine, risulta utile istituire, indicare nell'informativa e presidiare un account di posta elettronica dedicato, individuando un soggetto che - all'interno dell'organizzazione dello studio professionale - riscontri le istanze degli interessati, in accordo con il titolare del trattamento, entro massimo 30 giorni dal ricevimento della richiesta, così come previsto dall'art. 12 GDPR.

[41] Cfr. art. 15, GDPR.
[42] Cfr. art. 12, par. 3, GDPR.

Commissioni di riproduzione[43]

Le informazioni fornite dal titolare sono in generale gratuite. Se, tuttavia, la richiesta dovesse risultare manifestamente infondata o eccessiva il titolare, che deve provare la sussistenza di una di queste condizioni, può:

a) addebitare un contributo spese ragionevole;

b) rifiutare di soddisfare la richiesta.

Modalità di comunicazione dei dati[44]

il GDPR prevede che se la persona inoltra una domanda per via elettronica, l'informazione richiesta è comunicata in forma elettronica di uso comune, a meno che l'interessato non richieda diversamente.

Il Regolamento prevede, inoltre, che il responsabile del trattamento assista il titolare nell'adempimento dei suoi obblighi riguardo al diritto di accesso[45].

Il professionista potrebbe chiedere l'assistenza al fornitore di servizi informatici (responsabile del trattamento) di assisterlo per il recupero dei dati personali presenti all'interno di un database.

Diritto di rettifica[46]

L'interessato ha diritto di chiedere la rettifica o l'integrazione dei propri dati personali e la richiesta deve essere soddisfatta dal titolare senza ingiustificato ritardo e comunque entro 1 mese dalla richiesta stessa.

Diritto alla cancellazione – diritto all'oblio[47]

L'art. 17 del GDPR prevede il diritto dell'interessato di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano ed il correlativo obbligo di adempiere senza ingiustificato ritardo da parte del titolare stesso.

Modalità di esercizio del diritto

[43] Cfr. art. 12, par. 5, GDPR.
[44] Cfr. art. 12, par. 3, GDPR.
[45] Cfr. art. 28, par. 3, lett. e), GDPR.
[46] Cfr. art. 16, GDPR.
[47] Cfr. art. 17, GDPR.

Prima di procedere alla cancellazione dei dati personali, il titolare effettua un controllo di proporzionalità tra gli interessi della persona interessata e quelle del titolare del trattamento o, se del caso, del pubblico in generale (diritto all'informazione o interesse storico).
L'interessato ha il diritto di chiedere che siano cancellati e non più sottoposti a trattamento i propri dati personali quando:
a) non siano più necessari per le finalità per le quali sono stati raccolti o altrimenti trattati;
b) quando abbia revocato il proprio consenso o sia venuto meno il motivo per cui sono stati forniti;
c) si è opposto al trattamento e non sussiste più alcun motivo legittimo prevalente;
d) i dati personali sono stati trattati illecitamente;
e) i dati personali devono essere cancellati in adempimento di un obbligo legale;

Limiti all'esercizio del diritto di cancellazione

L'esercizio del diritto di cancellazione cede il passo di fronte all'adempimento di alcuni obblighi di archiviazione dei dati per periodi specifici e risulta pertanto non utilmente esercitabile ove comprometta l'adempimento ad obblighi fiscali o si ponga in contrasto necessità archivistiche di pubblico interesse ovvero, infine, ove il mantenimento del dato sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria.

Diritto alla limitazione del trattamento[48]

A seguito dell'esercizio del diritto di limitazione da parte dell'interessato, il titolare può continuare a trattare i dati personali soltanto con il consenso dell'interessato o se è necessario per l'accertamento, l'esercizio o la difesa in diritto in sede giudiziaria o per motivi di interesse pubblico rilevante. Resta fermo il diritto del titolare di continuare a trattare i dati ai fini della conservazione.

Quando l'interessato può richiedere la limitazione del trattamento?

a) se l'interessato contesta l'esattezza dei dati;
b) se il trattamento è illecito e l'interessato chiede la limitazione del trattamento, opponendosi alla cancellazione prevista dall'art. 17, par. 1, lett. d), GDPR;

[48] Cfr. art. 18, GDPR.

c) l'interessato ha bisogno dei dati per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, nonostante il titolare non necessiti più di tali dati;
d) l'interessato ha esercitato il diritto di opposizione.

Diritto di opposizione[49]

Per motivi connessi alla sua situazione particolare, l'interessato può opporsi al trattamento dei dati personali quando la base giuridica del trattamento è:
a) l'interesse legittimo del titolare (art. 6, par. 1, lett. f), GDPR);
b) l'esecuzione di un compito di interesse pubblico (art. 6, par. 1, lett. e), GDPR).
Inoltre, l'interessato può opporsi al trattamento dei dati personali qualora i dati personali siano trattati per finalità di marketing diretto (compresa la profilazione, nella misura in cui sia connessa a tale marketing diretto)[50].

Conseguenze dell'esercizio del diritto di opposizione

A seguito dell'esercizio del diritto di opposizione, il titolare non potrà più trattare i dati personali a meno che:
a) non dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato;
b) il titolare debba utilizzare quei dati per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
Il diritto di opposizione deve essere portato all'attenzione dell'interessato in modo esplicito, chiaro e separato da ogni altra informazione e non oltre la prima comunicazione con l'interessato.

[49] Cfr. art. 21, GDPR.
[50] L'interessato può, altresì, opporsi al trattamento per motivi connessi alla sua situazione particolare, qualora i dati personali siano trattati ai fini di ricerca scientifica o storica o a fini statistici, salvo che il trattamento sia necessario per un compito di interesse pubblico.

Sicurezza dei dati personali

Le informazioni, anche quelle comprendenti dati che rientrano nel novero di quelli definiti come personali, ai sensi dell'art. 4 GDPR, rappresentano il patrimonio informativo che costituisce un valore fondamentale per un professionista o uno studio professionale. Tali informazioni possono essere contenute in database, cartelle di file, archivi cartacei, utilizzando supporti analogici (carta, fotografie, etc.) o digitali (chiavi USB, DVD, etc.) e trasmessi mediante posta tradizionale, telefono, reti informatiche, etc.

La sicurezza delle informazioni, quindi, non riguarda soltanto i dati in formato digitale e trattati mediante sistemi informatici (sicurezza informatica), ma tutti i sistemi utilizzati per raccogliere, modificare, conservare, trasmettere e cancellare tali dati, in qualsiasi forma siano trattati.

Garantire la sicurezza di tali sistemi permetterà di assicurare la sicurezza dei dati personali trattati, attenuando il rischio per i diritti e le libertà delle persone fisiche che potrebbe derivare dal trattamento dei dati personali, così come richiesto dall'art. 32, GDPR.

La gestione del rischio

In tutti i contesti, la gestione del rischio, cioè degli eventi che possono avere effetti negativi su determinati aspetti personali o patrimoniali, comporta la valutazione del rischio stesso mediante differenti fasi:

A. identificazione del rischio
B. analisi del rischio
C. ponderazione del rischio

Per valutare i rischi occorre prendere in considerazione i seguenti parametri:
1. il contesto;
2. l'asset e il suo valore;
3. il tipo di minaccia e la probabilità che si verifichi;
4. le vulnerabilità del sistema e la loro gravità;
5. i controlli di sicurezza e la loro robustezza.

In sintesi, quindi, si può dire che valutare i rischi significa identificarli (asset, minacce, vulnerabilità) calcolarne il livello e decidere le misure da adottare per scongiurarlo.

Valutazione del rischio e verifiche periodiche[51]

L'individuazione delle possibili minacce rispetto ai trattamenti effettuati permette al titolare di compiere una corretta valutazione del rischio.
Vediamo quali domande deve porsi il professionista in base all'area coinvolta

Risorse di rete e tecnologiche

1. Vi sono parti del trattamento svolte attraverso internet?
2. È possibile accedere a un sistema di trattamento dei dati attraverso Internet (per esempio, riguardo a certi utenti o gruppi di utenti)?
3. Il sistema di trattamento dati personali è interconnesso a un altro sistema o servizio IT interno o esterno allo studio?
4. È facile per soggetti non autorizzati accedere all'ambiente di trattamento dati?
5. Il sistema di trattamento dati personali è progettato, implementato o manutenuto seguendo le migliori pratiche del settore?

B. Processi e procedure

1. Ruoli e procedure relative al trattamento di dati personali sono definiti in modo adeguato?
2. L'utilizzo accettabile delle risorse di rete, di sistema e fisiche all'interno dello studio è definito in modo adeguato?
3. Ai dipendenti/collaboratori è consentito portare con sé e utilizzare i propri dispositivi collegandoli al sistema di trattamento dati personali?
4. Ai dipendenti/collaboratori è consentito trasferire, memorizzare o comunque trattare dati personali al di fuori del perimetro dell'ente?

[51] Cfr. "Manuale sulla Sicurezza nel trattamento dei dati personali" ENISA del dicembre 2017.

5. Le attività di trattamento dati personali possono essere svolte senza che ciò comporti la creazione di file di registrazione eventi (log files)?

C. Soggetti e persone coinvolte

1. Vi sono parti del trattamento svolte da un soggetto esterno (responsabile del trattamento)?
2. Gli obblighi dei soggetti/delle persone coinvolti nel trattamento di dati personali sono fissati in modo adeguato?
3. Il personale che partecipa al trattamento di dati personali ha conoscenze in materia di sicurezza delle informazioni?
4. I soggetti/le persone che partecipano al trattamento di dati personali seguono delle policy sulla conservazione (data retention) e sulla cancellazione dei dati personali?

D. Valutazione del rischio

1. Ritiene che il proprio settore di attività sia passibile di attacchi cibernetici (cyberattacks)?
2. Lo studio ha subito attacchi cibernetici o altre tipologie di violazioni della sicurezza negli ultimi due anni?
3. Sono stati ricevuti notifiche e/o reclami relativamente alla sicurezza dei sistemi IT (utilizzati per il trattamento di dati personali) nell'ultimo anno?
4. Un trattamento riguarda volumi consistenti di dati personali e/o un numero consistente di persone fisiche?
5. Esistono migliori pratiche in materia di sicurezza specifiche del settore di attività dello studio che non siano state implementate in misura adeguata?
6. È stato valutato l'impatto legale, economico e reputazionale che un data breach[52] (violazione di sicurezza) può avere sullo studio?

Oltre alle suddette valutazioni, il titolare dovrebbe prendere in considerazione:

1. lo stato delle misure di sicurezza, tecnologiche e organizzative dello studio;
2. quali siano le diverse categorie di dati personali gestiti dallo studio, in modo da definire rispettivamente un adeguato livello di protezione;

[52] Sulla definizione e la gestione di un data breach si veda il capitolo "Sicurezza dei processi organizzativi".

3. la ripetizione periodica della valutazione dei rischi (almeno una volta/anno).

Misure di sicurezza

Una volta accertati, analizzati e ponderati i rischi, è possibile adottare le adeguate misure tecniche e organizzative, ossia i processi, le politiche e le prassi che permettono o dovrebbero permettere l'annullamento o la mitigazione dei rischi individuati, assicurando in particolare:

- la riservatezza (*confidentiality*) dei dati, ossia la proprietà di un'informazione di non essere disponibile o rivelata a soggetti o organizzazioni non autorizzate;
- l'integrità (*integrity*) dei dati, che riguarda la loro accuratezza e completezza;
- la disponibilità (*availability*) dei dati, cioè la loro accessibilità e utilizzabilità su richiesta di uno o più soggetti autorizzati.

Il principio di *accountability* non consiste nell'adesione burocratica a regole e schemi rigidamente impartiti, ma nella determinazione delle strategie più efficaci ad assicurare la sicurezza del trattamento, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel Regolamento.

Le indicazioni operative che seguono servono a dare al professionista gli strumenti di base per garantire un trattamento dei dati personali in sicurezza, ma non potranno eliminare completamente i rischi, né possono essere considerate principi assoluti: ciascun professionista è tenuto a valutare i rischi della propria attività e adottare efficaci misure di sicurezza in ragione:

- dello stato dell'arte;
- dei costi di attuazione;
- della natura, oggetto, contesto e finalità del trattamento.

Gestione degli archivi cartacei

La digitalizzazione dei processi e delle attività, che quotidianamente si compiono nello svolgimento della professione, non ha fatto venir meno il trattamento dei dati personali mediante l'uso della carta e la loro organizzazione in archivi cartacei.

La gestione dei dati personali in forma analogica è un aspetto che non va assolutamente trascurato, così come l'adeguatezza della struttura rispetto a eventi (incendio, intrusione, etc.) che possono incidere sulla riservatezza, l'integrità o la disponibilità dei dati (personali).

Anche il semplice cartiglio relativo ad una perizia estimativa, svolto senza l'ausilio di strumenti automatizzati, rappresenta pur sempre un trattamento di dati personali ai sensi dell'art. 4, par. 2, GDPR.

Una volta individuati e classificati i dati personali trattati, distinguendo fra dati personali "comuni" e particolari categorie di dati (ai sensi dell'art. 9, p. 1, GDPR) è possibile seguire le seguenti regole:

- i documenti contenenti dati personali appartenenti a particolari categorie devono essere conservati in armadietti chiusi a chiave il cui accesso è limitato a un determinato numero di persone all'interno dello studio;
- i dati personali "comuni" possono essere conservati in scaffalature a giorno all'interno di faldoni, o altro tipo di contenitore (ad es. i tubi per i disegni), a condizione che non si trovino in luoghi aperti al pubblico o comunque non presidiati.

È preferibile evitare di scrivere sulle etichette dei faldoni dati personali riferibili al cliente, essendo sufficiente un codice identificativo o il nome del progetto.

Sul piano organizzativo, è utile dotarsi di un distruggi-documenti all'interno dello studio, per procedere alla distruzione definitiva dei documenti cartacei contenenti dati personali, una volta superati i limiti temporali di conservazione dei dati personali e decorso il tempo prescritto dalla legge per la conservazione dei documenti in questione.

Sicurezza fisica

Sicurezza della sede

Gli uffici e le aree di uno studio professionale, specie quelli più complessi, andrebbero disposti in base al tipo di dati trattati e al livello di rischio: nei pressi dell'ingresso gli uffici dove sono trattati i dati personali "comuni" e via via che ci si allontana dall'ingresso, gli uffici che trattano particolari categorie di dati e le aree dove sono ubicati server e apparecchiature informatiche.

Controllo degli accessi alla sede e agli uffici

Negli Studi maggiormente strutturati sarebbe buona pratica richiedere alle persone che accedono alle proprie sedi di tenere in vista un tesserino (*badge*), in modo da riconoscere il personale interno, i fornitori abituali e i clienti. A questi, compresi gli addetti alle pulizie, dovrebbero essere fornite regole di comportamento fra le quali: tenere il tesserino in vista, non permettere ad altre persone di accedere alla sede o agli uffici, specie quando asseriscono di aver dimenticato le chiavi o il tesserino.

Per evitare intrusioni si possono utilizzare meccanismi tradizionali (cc.dd. passivi), come le grate alle finestre, e sistemi di rilevamento delle intrusioni e di allarme (cc.dd. attivi).

È buona norma chiudere a chiave l'ufficio quando ci si assenta e vi è il rischio che soggetti non autorizzati possano accedere ai dati personali.

Per i sistemi di videosorveglianza è sempre necessario seguire quanto prescritto dalle normative relative al trattamento dei dati personali e alla tutela dei lavoratori (art. 4, L. 300/1970 – Statuto dei Lavoratori): segnalare la presenza delle telecamere, controllare gli accessi ai monitor e alle registrazioni, cancellarle dopo alcuni giorni, stipulare un previo accordo sindacale qualora il sistema di videosorveglianza possa comportare un controllo a distanza dell'attività dei lavoratori.

Sicurezza delle apparecchiature informatiche

Le apparecchiature possono essere server, pc e altri dispositivi informatici e strumenti di ufficio come stampanti o fax.

Le apparecchiature dovrebbero essere disposte su pavimenti flottanti, a distanza da condutture di liquidi, in locali ad accesso limitato per evitare l'ingresso di estranei e i danni dovuti a disattenzione e con rilevatori di fumo e di allagamento e sistemi di spegnimento degli incendi.

Per evitare il danneggiamento delle apparecchiature e la perdita di dati personali (disponibilità) si consiglia di utilizzare UPS (*uninterruptible power supply*) e batterie tampone.

Dismissione delle apparecchiature

Tutte le apparecchiature informatiche (PC, stampanti, scanner, fax, cellulari, tablet e memorie esterne), quando dismesse, assegnate a un nuovo utilizzatore o consegnate a un fornitore, devono essere opportunamente ripulite da dati o informazioni riservate.

Per evitare il recupero dei dati cancellati, è necessario modificare tutti i bit del supporto di memoria con dei software di *wiping* o *erasing*[53].

Particolare attenzione va posta su certe tecnologie (per esempio i dischi SSD) per cui i normali sistemi di *wiping* non sono sufficienti.

Gli hard disk più recenti potrebbero addirittura subire dei danni da attività di *wiping*: un'unica sovrascrittura è sufficiente.

Metodi alternativi prevedono la smagnetizzazione della memoria con un *degausser* o la distruzione fisica, ma in quest'ultimo caso non sarà possibile, ovviamente, il riutilizzo della memoria.

Sicurezza delle tecnologie e degli strumenti informatici

Possedere tecnologie aggiornate ed efficienti è il primo passo per minimizzare gli effetti di un attacco informatico e proteggere i dati personali posseduti. I concetti di seguito descritti, pur non approfondendo i risvolti strettamente tecnici, sono utili al professionista per acquisire gli strumenti necessari al riconoscimento di un rischio, al fine di valutarlo e richiedere, eventualmente, l'assistenza di un esperto IT, interpellandolo correttamente e dunque essendo in grado di seguirlo nell'attività da svolgere.

Tuttavia, un elemento fondamentale per incrementare i livelli di sicurezza nell'utilizzo degli strumenti informatici nello studio professionale è la predisposizione di apposite policy o regolamenti sull'utilizzo degli strumenti e delle risorse informatiche dello studio professionale che i collaboratori/dipendenti siano tenuti a rispettare.

[53] I file cancellati non sono realmente rimossi in modo definitivo, ma deallocati. La traccia informatica rimane conservata sul disco rigido e finché i dati non saranno sovrascritti sarà sempre possibile recuperarli servendosi di software dedicati.

Mantenere i software aggiornati

Anche il mancato aggiornamento di un software risulta essere una delle potenziali vulnerabilità che possono essere sfruttate per sottrarre informazioni, dati personali, attivare la webcam, il microfono, leggere le parole digitate sulla tastiera, tutto all'insaputa dell'utilizzatore.

Azioni da intraprendere:

- Acquistare antivirus di livello e software per filtrare le mail;
- Assicurarsi di aggiornare il sistema operativo (Windows, Mac OS X, Linux), verificando la disponibilità di aggiornamenti o il rilascio di nuove versioni e solo da fonti ufficiali (ad. es. Windows Update). È preferibile impostare l'aggiornamento automatico del suddetto sistema operativo;
- Assicurarsi che gli aggiornamenti del firmware siano effettuati non solo sui PC, ma anche sui modem e i router;
- Effettuare la scansione antivirus automatica di tutti gli allegati alle e-mail, senza lasciare questo compito agli utenti.

Protezione degli endpoint

Qualunque dispositivo connesso alla rete dello studio (PC, smartphone, stampante, ecc.) è un endpoint. Tramite queste "porte" entrano ed escono i dati dalla rete verso internet: è fondamentale che siano adeguatamente protette e monitorate.

Azioni da intraprendere:

- Implementare protezioni antivirus e firewall che filtrino un certo tipo di traffico di rete al fine di proteggere i sistemi informatici e tenere traccia del traffico.

Utilizzare connessioni internet sicure

Accedere a reti Wi-Fi poco sicure (come quelle di alberghi, bar, ristoranti, aeroporti) significa essere esposti alla probabile intercettazione dei dati personali e/o informazioni strategiche da parte dei cybercriminali.

Qualora i dipendenti o i collaboratori lavorino da remoto (ad esempio a casa o durante una trasferta), devono accertarsi che la connessione utilizzata sia sicura, utilizzando una virtual private network (VPN) e non una connessione Wi-Fi pubblica. Una VPN è una connessione cifrata, una sorta di tunnel virtuale all'interno della rete utilizzata e può essere creata con l'utilizzo di semplici software o app.

Sicurezza del browser e delle e-mail

Le e-mail e la navigazione Internet sono i due principali vettori utilizzati dagli hacker per effettuare un attacco.

Azioni da intraprendere:

- Aggiornare costantemente il browser utilizzato (Chrome, Firefox, Safari, Microsoft Edge o Internet Explorer, ecc.);
- Disabilitare la funzione di auto-completamento/auto-riempimento;
- Disabilitare la connessione a internet di computer o server quando non necessaria;
- Non utilizzare caselle di posta elettronica gratuite. Sono senz'altro da preferire servizi a pagamento generalmente riconosciuti.

Crittografare dati e dispositivi

La crittografia è una tecnica che permette di rendere illeggibili i file a chi non possiede la password o la chiave per decriptarli. Possono essere criptati sia file contenuti in un dispositivo o hard disk, sia file trasmessi telematicamente (v. la VPN).

Azioni da intraprendere:

- Criptare file contenenti dati personali appartenenti a categorie particolari o relativi a condanne penali o reati[54];
- Criptare tutte le cartelle in cui sono archiviati dati appartenenti a categorie particolari;
- Cercare di limitare l'accesso ai dati più importanti solo ai collaboratori autorizzati o ai dispositivi necessari.

[54] Di cui, rispettivamente, agli artt. 9 e 10 del GDPR.

Cifratura e pseudonimizzazione[55]

La cifratura è una tecnica che permette di rendere illeggibili i dati contenuti in un hard-disk a meno che non si conosca la relativa chiave (password). Il GDPR consiglia di adottare questa misura tecnica a protezione dei dati personali, ma esistono diverse tecniche di cifratura e non tutte garantiscono lo stesso livello di protezione. Per questo il professionista che intende adottare la cifratura a protezione dei dati personali trattati deve scegliere la migliore possibile in relazione alle proprie esigenze e al proprio contesto.

Per pseudonimizzazione s'intende "*il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative* (es. cifratura) *intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile*"[56].

Cancellazione da remoto

È abbastanza frequente che si verifichi la perdita o la sottrazione di uno smartphone, di un PC o di altro dispositivo. Nel caso in cui il dispositivo non sia crittografato è sempre possibile installare un software in grado di cancellare alcuni o tutti i file da remoto, a patto che il software sia già presente nel dispositivo prima dello smarrimento/sottrazione.

Azioni da intraprendere:

- Installare un software per la cancellazione dei dati da remoto. Il software opererà soltanto se il dispositivo è connesso ad internet.

[55] Cfr. art. 32, par. 1, lett. a), GDPR.
[56] Così art. 4, n. 5), GDPR.

Cloud Computing

Molto sinteticamente e genericamente, il cloud computing consiste nell'erogazione di servizi (software, app, storage, e-mail) da parte di un provider a richiesta di un cliente attraverso la rete internet e resi disponibili su risorse server in remoto.

Azioni da intraprendere:

- Assicurarsi che i dati dei clienti siano memorizzati in un luogo soggetto alla medesima giurisdizione alla quale è soggetto il titolare del trattamento. Questo perché molti Stati consentono a terze parti (soprattutto autorità governative) di controllare i dati dei cittadini e delle organizzazioni private, compromettendo così anche la riservatezza dei loro clienti;
- Assicurarsi che il provider implementi politiche di sicurezza adeguate;
- Verificare se i dati sono memorizzati con sistemi di crittografia, ove necessario;
- Verificare quali siano i sistemi di autenticazione al cloud e se è possibile l'autenticazione a due fattori (es. pin + token);
- Assicurarsi che il provider effettui regolarmente dei back-up e verificare quale sia la politica di conservazione dei dati (c.d. *data retention*).

Gestione del controllo degli accessi

Il controllo degli accessi riguarda il diritto riconosciuto ad alcuni individui di accedere a tutta o parte della rete internet dello studio professionale, ma anche alle risorse e ai file che possono essere gestiti su storage condivisi.

Azioni da intraprendere:

- Ridurre al minimo gli account amministratore (quelli che hanno accesso completo a tutte le risorse);
- Individuare quali risorse necessitino del livello di autorizzazione più elevato e utilizzare profili amministrativi specifici con privilegi ridotti;
- Restringere l'accesso ai documenti e alle risorse ai soli utenti che ne hanno bisogno per svolgere i propri compiti;

- Bloccare prontamente l'accesso ai collaboratori/dipendenti che non fanno più parte dello studio, per evitare accessi non autorizzati da remoto.
- Predisporre delle apposite policy o regolamenti sull'utilizzo degli strumenti e delle risorse informatiche dello studio professionale che i collaboratori/dipendenti siano tenuti a rispettare.

Sicurezza dei dispostivi mobili

È indubbio che negli ultimi anni si sia assistito a un incremento notevole dei dispositivi mobili per svolgere le attività professionali, sia personali (c.d. BYOD, bring your own device) sia aziendali. Essi, tuttavia, contengono dati personali sia dell'utilizzatore del dispositivo, sia relativi alle attività dello studio professionale. Pertanto, è consigliabile adottare delle misure a tutela della sicurezza dei dati trattati anche tramite questa modalità.

Azioni da intraprendere:

- Redigere una policy sull'uso dei BYOD che definisca chiaramente le condizioni e i limiti dell'utilizzo dei dispositivi mobili nell'attività professionale;
- Utilizzare una soluzione MDM (Mobile Device Management) per proteggere i dati dello studio professionale. Se possibile, preferire soluzioni che separino i dati personali dell'utilizzatore del dispositivo da quelli relativi alle attività dello studio professionale;
- Se si utilizza il dispositivo personale (circostanza molto frequente) per l'attività professionale, definire delle impostazioni di sicurezza rigorose per assicurare un ambiente di lavoro sicuro (ad es. una password di accesso robusta, un meccanismo di scadenza della password, blocco dell'accesso al dispositivo trascorso un certo tempo e la crittografia del dispositivo).

Gestione dei processi organizzativi

Valutazione d'impatto sulla protezione dei dati (DPIA)[57]

Nel caso in cui un trattamento possa comportare un rischio elevato per i diritti e le libertà delle persone interessate (qualora vi sia un monitoraggio sistematico dei loro comportamenti o per il gran numero di soggetti interessati – c.d. trattamento su larga scala – di cui sono trattati, ad esempio, dati appartenenti a categorie particolari o relativi a condanne penali o reati), il GDPR obbliga il titolare a svolgere una valutazione di impatto prima di dare inizio al trattamento.
Qualora residui un rischio elevato per i diritti e le libertà degli interessati, nonostante il titolare abbia individuato le misure tecniche ed organizzative per attenuarlo, sarà necessario consultare l'autorità di controllo (Autorità garante per la protezione dei dati personali).

Quando è obbligatoria una DPIA?

In tutti i casi in cui un trattamento possa presentare un rischio elevato per i diritti e le libertà degli interessati. Tra questi:
- Trattamenti valutativi o di scoring, compresa la profilazione;
- Decisioni automatizzate che producono significativi effetti giuridici;
- Monitoraggio sistematico (es. videosorveglianza);
- Trattamento su larga scala di dati appartenenti a categorie particolari o relativi a condanne penali o reati;
- trattamenti su larga scala di dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, anziani, richiedenti asilo, ecc.);
- Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es. riconoscimento facciale, device IoT, ecc.).

Quando non è obbligatoria una DPIA?

Non è obbligatoria una DPIA per i trattamenti che:
- Non presentino un rischio elevato per i diritti e le libertà degli interessati;

[57] Cfr. art. 35, GDPR.

- Abbiano natura, ambito, contesto e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA;
- Siano stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio del 2018 e le cui condizioni (es. soggetto, finalità, ecc.) non abbiano subito modifiche;
- Facciano riferimento a norme e regolamenti, dell'Unione europea o di uno Stato membro, per la cui definizione sia stata condotta una DPIA.

Nei casi in cui non è chiaro se sia richiesta una valutazione d'impatto sulla protezione dei dati o meno, il WP29[58] raccomanda di effettuarla comunque, in quanto detta valutazione è uno strumento utile che assiste i titolari del trattamento a rispettare la legge in materia di protezione dei dati. Essa è particolarmente importante quando viene introdotta una nuova tecnologia di trattamento dei dati

La DPIA deve essere condotta prima di procedere al trattamento, prevedendo, comunque, un riesame a intervalli regolari.
responsabile della DPIA è sempre il titolare, anche se la conduzione della stessa può essere affidata a un soggetto terzo, esterno o interno allo studio. Il titolare monitora lo svolgimento della DPIA, consultandosi con il DPO (se presente) e, laddove necessario, richiedendo il parere di esperti del settore.

Data breach (artt. 33 e 34 GDPR)

In caso di una 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, il GDPR prescrive al titolare determinati comportamenti.

Alcuni esempi di data breach:
- Furto o perdita di dispositivi informatici contenenti dati personali;
- L'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- La divulgazione non autorizzata di dati personali;

[58] Cfr. "Linee-guida del Gruppo Articolo 29 in materia di valutazione di impatto sulla protezione dei dati (WP248)".

- L'impossibilità, anche temporanea, di accedere ai dati per cause accidentali o per attacchi esterni, virus, ecc.;
- La modifica o la cancellazione, non autorizzate o accidentali, di dati personali;
- L'invio di una comunicazione e-mail contenente dati personali a destinatari errati.

Comportamenti da tenere in caso di data breach

1. Notifica al Garante

Soggetto tenuto a effettuarla

Il titolare del trattamento. L'eventuale responsabile del trattamento coinvolto è tenuto a informare tempestivamente il titolare una volta venuto a conoscenza della violazione.

Quando

Senza ingiustificato ritardo e comunque entro 72 ore dal momento in cui il titolare è venuto a conoscenza della violazione. Trascorso questo intervallo di tempo, il titolare dovrà giustificare i motivi del ritardo all'atto della notifica all'Autorità Garante per la protezione dei dati personali.

Eccezioni

Non è richiesta la notifica all'Autorità Garante qualora sia improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche.

Tipi di violazioni di dati personali da notificare

Tutte quelle tipologie che possono avere effetti avversi significativi sugli individui, causando danni fisici, materiali e/o immateriali.

Quali informazioni deve contenere la notifica al Garante e come inviarla

La notifica deve contenere le informazioni previste all'art. 33, par. 3 del GDPR. Qualora si utilizzi per la notifica il modello predisposto dal Garante, è necessario scaricarlo sul proprio dispositivo e successivamente procedere alla sua compilazione.

La notifica deve essere inviata al Garante tramite posta elettronica all'indirizzo **protocollo@pec.gpdp.it** e deve essere sottoscritta digitalmente (con firma elettronica qualificata/firma digitale) ovvero con firma autografa. In quest'ultimo caso la notifica deve essere presentata unitamente alla copia del documento d'identità del firmatario.

2. Comunicazione agli interessati.

Se la violazione comporta un rischio elevato per i diritti delle persone, il titolare deve comunicarla anche a tutti gli interessati, utilizzando i canali più idonei, a meno che abbia già preso misure tali da ridurne l'impatto.

3. registro delle violazioni.

Tutte le volte in cui si verifica una violazione, a prescindere dalla notifica all'Autorità Garante, il titolare del trattamento deve documentarla predisponendo un apposito registro, al fine di consentire all'Autorità di effettuare eventuali controlli sul rispetto della normativa.

4. Formazione e test

Ai fini della prevenzione di eventuali data breach, è necessario:

- Organizzare corsi di formazione periodici e iniziative di sensibilizzazione per tutti i dipendenti/collaboratori sui temi della protezione dei dati personali;
- Effettuare stress test e altre valutazioni di impatto delle minacce per testare la sicurezza e i tempi di risposta, almeno una volta l'anno.

Assicurazione per la responsabilità da attacchi informatici

Anche se uno studio professionale implementa i migliori processi e tecnologie di sicurezza informatica, resterà comunque esposto a un certo livello di rischio.

Pertanto, dopo aver valutato l'esposizione al rischio, si dovrebbe prendere in considerazione una polizza assicurativa che copra il rischio residuo di attacchi informatici, in modo da sostenere i costi di un eventuale *data breach*.

Formazione del personale

Le persone sono spesso l'anello debole nella sicurezza informatica. La mancanza di conoscenze o la semplice disattenzione sono elementi che i cybercriminali sfruttano a loro vantaggio. La maggior parte degli attacchi sono predisposti utilizzando comunicazioni apparentemente innocue o di routine, ma che in realtà contengono link attraverso cui possono essere ottenute informazioni riservate, quali username, password, dettagli sulle carte di credito. Gli hacker

preferiscono questo tipo di attacchi perché sono molto più efficienti rispetto alla violazione dei sistemi di sicurezza di un PC o di una rete.

Per questa ragione è fondamentale che tutti i membri di uno studio professionale conoscano le forme più comuni di un attacco informatico e siano formati per rispondere adeguatamente a tali attacchi. Se possibile, sarebbe utile testare il personale con simulazioni di *phishing* e verificare quale sia il livello di consapevolezza rispetto alla sicurezza informatica.

Inoltre, occorre considerare che i dipendenti e i collaboratori dello studio professionale, in qualità di autorizzati al trattamento ai sensi dell'art. 29 del GDPR, devono obbligatoriamente ricevere le adeguate istruzioni e la formazione necessaria al corretto trattamento di dati personali, nell'esecuzione delle prestazioni lavorative.

In effetti, l'obbligo di fornire le adeguate istruzioni agli autorizzati al trattamento e la necessaria formazione in materia di protezione di dati personali ricade espressamente in capo al titolare del trattamento, ai sensi del citato art. 29 GDPR.

La formazione del personale dello studio professionale, dunque, oltre alle norme del GDPR e alle necessarie istruzioni per procedere al corretto trattamento dei dati personali, dovrebbe avere ad oggetto anche le regole della sicurezza informatica.

Il personale deve essere consapevole che:

- I dati memorizzati nelle banche dati, comprese quelle degli studi professionali, acquisiscono sempre maggior valore e gli attacchi informatici si fanno più sofisticati e frequenti;
- Gli attacchi informatici potrebbero avere delle implicazioni legali, a causa del fatto che i professionisti sono tenuti a rispettare la riservatezza dei dati relativi ai loro clienti o di cui sono venuti in possesso nello svolgimento dell'attività professionale;
- Sussistono dei rischi di natura economica e reputazionale associati a una violazione della sicurezza informatica;
- Occorre essere formati per rispondere a un attacco informatico ed evitare perdite future.

Adozione di una policy sul corretto uso degli strumenti informatici

Al fine di garantire la massima trasparenza informativa ed evitare controlli occulti sull'attività lavorativa dei dipendenti/collaboratori, vietati dall'art. 4, L. 300/1970 (c.d. Statuto dei

Lavoratori), le misure di sicurezza tecniche e organizzative devono essere accompagnate dalla redazione e messa a disposizione di tutti i dipendenti/collaboratori di un disciplinare interno, scritto in un linguaggio chiaro, senza far ricorso a formule generiche e periodicamente aggiornato.

Sulla scorta di quanto stabilito dalle Linee guida per posta elettronica e internet del Garante per la protezione dei dati personali del 1° marzo 2007, il disciplinare interno deve specificare, a seconda dei casi:

- se determinati comportamenti non sono tollerati quando si naviga in internet (ad es. il download di software o file musicali, l'utilizzo di programmi per il download di contenuti protetti da diritto d'autore come *torrent*, etc.);
- in quale misura è consentito utilizzare anche per ragioni personali servizi di posta elettronica o di rete, anche solo da determinate postazioni di lavoro o caselle oppure ricorrendo a sistemi di *webmail*, indicandone le modalità e l'arco temporale di utilizzo (ad es., fuori dall'orario di lavoro o durante le pause, o consentendone un uso moderato anche nel tempo di lavoro);
- quali informazioni sono memorizzate temporaneamente (ad es., le componenti di *file di log*, eventualmente registrati) e chi, anche dall'esterno, vi può accedere legittimamente;
- se il datore di lavoro si riserva di effettuare controlli in conformità alla legge, anche saltuari o occasionali, indicando le ragioni legittime (sempre specifiche e mai generiche) per cui verrebbero effettuati e le relative modalità, precisando se, in caso di abusi singoli o reiterati, vengono inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispostivi o prestazioni;
- quali conseguenze, anche di tipo disciplinare, il datore di lavoro si riserva di trarre qualora accerti che la posta elettronica e internet siano utilizzati indebitamente;
- le soluzioni prefigurate per garantire, con la cooperazione del lavoratore, la continuità dell'attività lavorativa in caso di assenza del lavoratore stesso (specie se programmata), con particolare riferimento all'attivazione di sistemi di risposta automatica ai messaggi di posta elettronica ricevuti.

Alcuni esempi di minacce comuni

Il personale deve conoscere i differenti tipi di attacco informatico che potrebbero trovarsi ad affrontare con maggiore frequenza in uno studio professionale. Fra questi si ricordano:

- Malware: software malevoli come virus, worms, trojan horses, spyware e adware;
- Ransomware: questi software sono in grado di criptare o bloccare i dati e successivamente viene chiesto un pagamento (in genere in bitcoin) per ottenere la chiave di cifrature e accedere nuovamente ai dati;
- Phishing/spear phishing/whaling emails: si tratta di attacchi realizzati attraverso mail apparentemente legittime, contenenti link infettati con un malware o che cercano di carpire informazioni personali o finanziarie dal destinatario;
- Attacchi denial-of-service (DoS): attacchi informatici in cui si sovraccarica un dispositivo con un numero elevato di richieste fino a renderlo inutilizzabile;
- Furto di identità digitale: l'identità digitale è l'insieme dei dati informatici che identificano in maniera univoca una persona fisica, giuridica o un dispositivo online. Sfruttando la tecnica del *phishing*, un hacker potrebbe utilizzare l'account di un professionista e indurre un altro soggetto a effettuare un pagamento.
- Vulnerabilità cc.dd. zero-day: si tratta di vulnerabilità del codice di un software non ancora conosciute e che possono essere sfruttate dagli hacker che per primi le scoprono.

Sanzioni

La violazione delle disposizioni sul corretto trattamento dei dati personali comporta l'applicazione di sanzioni amministrative e penali.

Le sanzioni amministrative sono previste dal GDPR all'art. 83, quelle penali da diverse norme del Codice per la protezione dei dati personali (o "Codice privacy").

Le tabelle che seguono mostrano le violazioni in cui possono incorrere più frequentemente i Professionisti, le relative norme del GDPR e/o del Codice per la protezione dei dati personali violate e le sanzioni previste.

Violazioni	Sanzioni
Principi di privacy by design e by default (art. 25, GDPR)	Sanzione amministrativa 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, par. 4, GDPR)
Contitolarità (art. 26, GDPR)	
responsabile del trattamento (art. 28, GDPR)	
Trattamento svolto sotto l'autorità del titolare del trattamento o del responsabile del trattamento (art. 29, GDPR)	
Registri delle attività di trattamento (art. 30, GDPR)	
Cooperazione con l'autorità di controllo (art. 31, GDPR)	
Sicurezza del trattamento (art. 32, GDPR)	
Notifica di una violazione dei dati personali all'interessato (art. 33, GDPR)	
Comunicazione di una violazione dei dati personali all'interessato (art. 34, GDPR)	
Valutazione d'impatto sulla protezione dei dati (art. 35, GDPR)	

Violazioni	Sanzioni amministrative
Principi applicabili al trattamento dei dati personali (art. 5, GDPR)	Sanzione amministrativa fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83, par. 5, GDPR)
Liceità del trattamento (art. 6, GDPR)	
Condizioni per il consenso (art. 7, GDPR)	
Trattamento di particolari categorie di dati (art. 9, GDPR)	
Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato (art. 12, GDPR)	
Informazioni da fornire qualora i dati siano raccolti presso l'interessato (art. 13, GDPR)	
Informazioni da fornire qualora i dati non siano raccolti presso l'interessato (art. 14, GDPR)	
Diritto di accesso dell'interessato (art. 15, GDPR)	
Diritto di rettifica (art. 16, GDPR)	
Diritto di cancellazione (art. 17, GDPR)	
Diritto di limitazione al trattamento (art. 18, GDPR)	
Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazioni del trattamento (art. 19, GDPR)	
Diritto alla portabilità (art. 20, GDPR)	
Diritto di opposizione (art. 21, GDPR)	
Poteri dell'Autorità di controllo (art. 58, par. 1 e 2, GDPR)	

Violazioni	Sanzioni amministrative
Redazione dell'informativa in un linguaggio chiaro e semplice per il minore (art. 2, quinquies, c. 2, Codice privacy)	Art. 166, c. 2, D.lgs. 196/2003: si applica l'art. 35, par. 5, GDPR: sanzione amministrativa fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore
Trattamento dei dati relativi a studenti (art. 96, Codice privacy)	
Trattamento nell'ambito del rapporto di lavoro (artt. 111 e 111-bis, Codice Privacy)	
Accertamenti e controlli (art. 157, Codice Privacy)	

Violazioni	Sanzioni penali
Trattamento illecito dei dati personali	Reclusione da 6 mesi a 1 anno e 6 mesi (art. 167, Codice Privacy)
Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala	Reclusione da 1 a 6 anni (art. 167-bis, Codice privacy)
Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala	Reclusione da 1 a 4 anni (art. 167-ter, Codice privacy)
Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione o dell'esercizio dei poteri del Garante	Reclusione da 6 mesi a 3 anni (art. 168, Codice privacy)
Inosservanza dei provvedimenti del Garante	Reclusione da 3 mesi a 2 anni (art. 170, Codice privacy)
Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori	Ammenda da 154 euro a 1.549 euro o arresto da 15 giorni a 1 anno (art. 171, Codice privacy)

INFOGRAFICA