e-book

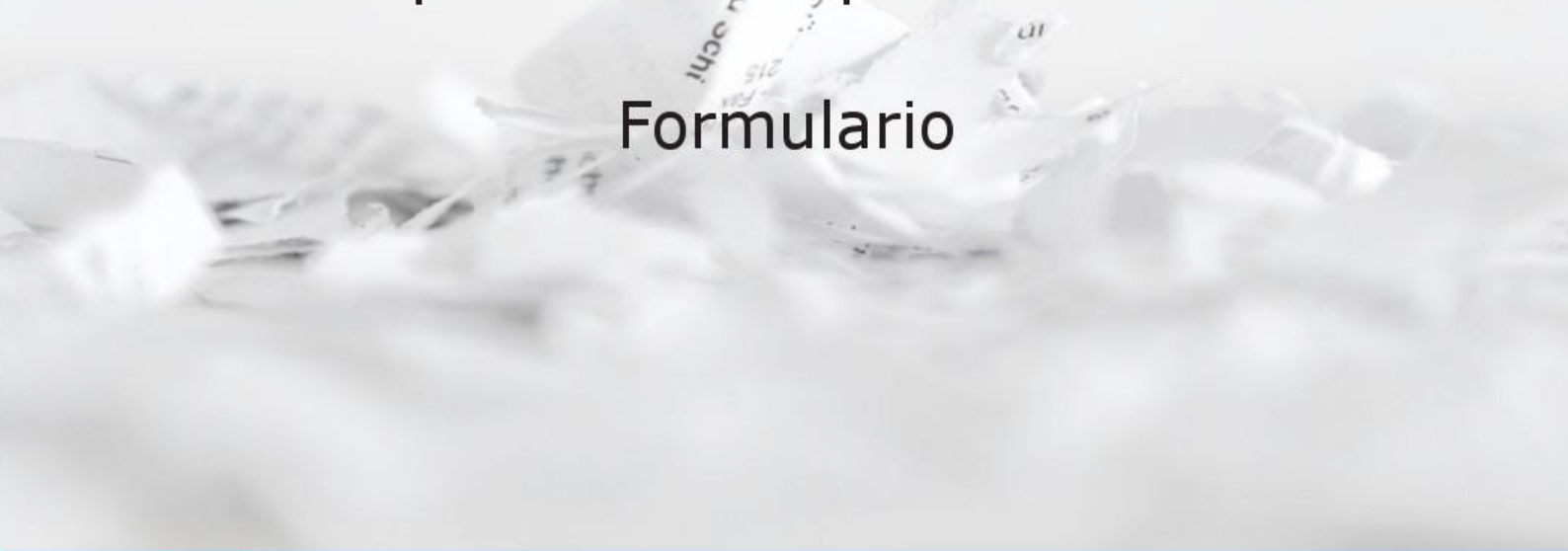
A cura di Giuseppe Miceli
Autori: Giuseppe Miceli, Marco Miceli, Luca Malatesta

LA PRIVACY NEGLI STUDI PROFESSIONALI

Schemi riepilogativi e consigli pratici per gli adempimenti

Focus operativo su ispezioni e sanzioni

Formulario



ORDINE AVVOCATI DI ROMA
FISCO eTASSE .com
la tua guida per un fisco semplice
MAGGIOLI EDITORE

A cura di Giuseppe Miceli

Autori: Giuseppe Miceli, Marco Miceli, Luca Malatesta

LA PRIVACY NEGLI STUDI PROFESSIONALI

Schemi riepilogativi e consigli pratici per gli adempimenti

Focus operativo su ispezioni e sanzioni

Formulario

ORDINE AVVOCATI DI ROMA

FISCO e TASSE .com
la tua guida per un fisco semplice

MAGGIOLI EDITORE

Dai colleghi, con i colleghi, per i colleghi.
Perché lo studio, la conoscenza,
la formazione sono i fari che devono guidare
l'avvocato nel suo percorso, illuminando
a sua volta con l'esempio il cammino
della società civile.

Antonino Galletti Presidente del Consiglio
dell'Ordine degli Avvocati di Roma

CONSIGLIO DELL'ORDINE DEGLI AVVOCATI DI ROMA
Palazzo di Giustizia – Piazza Cavour 00193 Roma

COMPONENTI IL CONSIGLIO DELL'ORDINE
QUADRIENNIO 2019/2022

PRESIDENTE

Antonino GALLETTI

VICEPRESIDENTE

Mauro MAZZONI

CONSIGLIERE SEGRETARIO

Mario SCIALLA

CONSIGLIERE TESORIERE

Alessandro GRAZIANI

CONSIGLIERI:

Angelica ADDESSI, Maria AGNINO, Alessia ALESII, Lucilla ANASTASIO, Riccardo BOLOGNESI, Antonio CAIAFA, Giorgia CELLETTI, Donatella CERE', Irma CONTI, Pietro DI TOSTO, Stefano GALEANI, Grazia Maria GENTILE, Enrico LUBRANO, Aldo MINGHELLI, Saveria MOBRICI, Paolo NESTA, Roberto NICODEMI, Andrea PONTECORVO, Matteo SANTINI, Cristina TAMBURRO, Paolo VOLTAGGIO

Giuseppe Miceli

Legal Advisor - Giurista abilitato alla professione forense.
Laureato presso l'Università degli studi di Roma *"La Sapienza"* con tesi di laurea in diritto processuale penale, dal titolo *"Prove penali e inutilizzabilità"*. Abilitazione alla professione di Avvocato nel 2008, presso la Corte d'Appello di Roma. Docente al Master "*Manager dei processi innovativi nelle start-up culturali e creative"* presso l'Università degli Studi Camerino*;* ai Master in *"Data Analyst"* e in *"Sicurezza delle reti informatiche"* dell'Università Niccolò Cusano. Relatore in numerosi convegni accreditati presso *l'Ordine degli Avvocati di Roma e Ancona e Ordine dei Consulenti del Lavoro di Roma.* Componente esterno, Esperto in materia di Antiriciclaggio, del Centro Studi dell'Ordine dei Consulenti del Lavoro di Roma.

Marco Miceli

Pluriennale esperienza nel mondo HR. Ha rivestito sin da giovane responsabilità presso multinazionali, gestendo importanti progetti e obiettivi.
Esperto conoscitore di tutte le tematiche HR come *recruiting*, selezione *&* formazione, riorganizzazioni e *star up* aziendali, *compensation*, gestione degli ambienti di lavoro, gestione della corretta applicazione delle normative legislative e contrattuali per il personale in materia di lavoro, fiscale, previdenziale e assistenziale, *welfare*, sviluppo e *change management*, *budgeting*, contrattazione aziendale e relazioni sindacali.
Attualmente *Reporting & Reporting Manager*, presso la Direzione Risorse Umane di un importante Gruppo che opera nell'ambito delle tecnologie avanzate ambito trasporti, coordina un *team* di risorse per importanti progetti internazionali.

Luca Malatesta

Avvocato con più di 15 anni di esperienza nella consulenza direzionale, forte del *background* nel campo delle telecomunicazioni e dell'informatica, si interessa della *compliance* delle grandi aziende internazionali e delle PMI italiane. Nel 2005 a lavorare alla figura del Global@ccount®, ovvero il consulente multidisciplinare. Più tardi crea *Insight*, piattaforma *software* proprietaria per la gestione di *audit* e *compliance* normativa e attorno alla piattaforma crea MBS - *My Business Solutions*, un coagulo di competenze ed eccellenze professionali, di cui è Amministratore e coordinatore delle direzioni scientifiche incaricate di trasformare il proprio know-how in valore aggiunto sulla piattaforma.

ISBN: 9788868058449
Ottobre 2019

www.fiscoetasse.com

Indice

Prefazione

Il 27 Aprile 2016 la Commissione Europea ha presentato il Regolamento 679/2016 per l'aggiornamento della normativa concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati. Il Regolamento UE, essendo un atto *self executive*, ai sensi dell'art. 288 del Trattato sul funzionamento della Comunità Europea, è direttamente esecutivo e non necessita di recepimento da parte degli stati membri, cosicchè a decorrere dal 25 Maggio 2018, la normativa succitata è diventata immediatamente applicabile anche nello Stato italiano. L'intero Regolamento 679/2016 è costellato da una costante dialettica tra tecnica e libertà, innovazione e diritti, iniziativa economica e garanzie. Significativa è l'esigenza di adeguamento della disciplina alla realtà nella sua evoluzione tecnologica. Non vi è dubbio, infatti, che tanto le norme giuridiche quanto le norme tecniche formano ormai un sistema fortemente interconnesso rispetto a qualunque uso corretto dei dati , in particolare con riguardo alla legittimità della raccolta, uso e conservazione di quelli personali ed è altrettanto vero che redigere una collettanea che descriva il rapporto tra nuove tecnologie e mondo giuridico è una sfida che si presenta impossibile da vincere per il rischio che le nozioni espresse diventino obsolete al momento della pubblicazione . Bene hanno fatto gli autori a proporre una pubblicazione snella, che trattasse ed avvicinasse i cittadini, siano essi professionisti o imprenditori, al mondo della protezione dei dati. Ciò che trasuda da questa collettanea è un grande senso di legalità e di conoscenza delle norme espresse in modo semplice e costruttivo e voglio augurarmi che in un futuro, spero prossimo, decidano di cimentarsi con altre sfide letterarie , li leggeremo sempre con piacere.

Giulio Botta

Presidente Associazione Europea Protezione Dati

Via Flaminia 392

60126 Ancona

Premessa
(Avv. Luca Malatesta)

A poco più di un anno dal 25 maggio 2018, termine ultimo per l'applicazione del Regolamento Generale Europeo Per La Protezione Dei Dati, che tutti ormai conosciamo attraverso l'acronimo inglese GDPR, la politica dei grandi numeri, delle grandi aziende e dei grandi gruppi lo sbandiera come un grande successo politico soprattutto in Europa. Il Regolamento, infatti, nella realtà delle imprese medio-grandi, globalizzate e mondiali è diventato lo standard di riferimento adottato tout-court "*dai paesi che costituiscono il 42% del PIL mondiale e il 34% degli scambi globali*[1]" con l'effetto molto pratico che chiunque abbia attività transnazionali di qualche tipo con un paese occidentale debba in qualche modo farci i conti.

La parte di più faticosa applicazione per un professionista regolamentato che operi sul mercato italiano e che debba lavorare per la conformità normativa del proprio studio professionale ovvero dell'attività di un cliente, secondo la personale esperienza di chi scrive, sta proprio nella struttura stessa della normativa.

Il legislatore europeo, infatti, nella redazione del Regolamento ha attinto a piene mani dai **paradigmi aziendali di "automiglioramento" e "autovalutazione" propri delle cosiddette normative volontarie**, come gli standard internazionali di qualità che pongono in capo al titolare del trattamento prima ancora che un obbligo di adeguamento a dei parametri normativamente previsti, il non facile compito di stabilire quali misure siano nel pratico sufficienti ed adeguate alla tutela dei dati che gli vengono affidati dall'interessato. Ne discende, sotto l'ombrello della responsabilizzazione del titolare, quel principio di *accountability* ormai entrato nel lessico comune degli operatori che abbiano a che fare con la riservatezza, una **grande difficoltà per l'operatore pratico**, tradizionalmente abituato a ritenere la *compliance* come una serie di esatti adempimenti che scaturivano dal dettato normativo del vecchio codice.

A questo deve aggiungersi anche il fatto che la lunga gestazione del GDPR ha fatto sì che le autorità politiche e di governo europee, in particolare alcune fossero soggette ad enormi pressioni di lobbying come denunciato dal Garante della Privacy Antonello Soro nella *lectio magistralis* tenuta all'Università di Firenze il 4 marzo 2019. Ne è uscita fuori una legislazione che, a parere di chi scrive, risulta

[1] Martin Selmayr, Segretario generale della Commissione Juncker, 16 mag 2019.

eccessivamente tagliata per le grandi aziende multinazionali, basti pensare all'istituto dell'*one-stop-shop* che permette ai colossi dell'informatica di scegliersi in pratica con quale garante nazionale avere un'interlocuzione privilegiata, mentre delega alle autorità garanti nazionali un'impressionante opera di *soft law* per promulgare regolamenti di dettaglio applicabili a singole categorie o fattispecie. Nell'attesa che le autorità garanti smaltiscano questo enorme carico di lavoro, il GDPR con tutto il suo apparato sanzionatorio è pienamente in vigore anche per i professionisti che dovranno **tradurre nella realtà** dei loro studi la normativa, in azioni concrete, anche senza necessariamente far ricorso a uffici *compliance* come quelli delle grandi aziende, ovvero costosi consulenti esterni.

Un approccio che può certamente aiutare nella pratica, nonostante la stragrande maggioranza dei contributi reperibili ponga il titolare del trattamento al centro di normative, azioni, contromisure, è porre l'accento, invece, sull'interessato.

Un titolare del trattamento, nel nostro caso il **professionista**, è infatti il **primo garante della regolarità del trattamento.** L'aderenza al GDPR comporta infatti la comprensione di tutta la serie di regole di condotta che il titolare deve all'interessato in cambio del conferimento dei suoi dati, a cominciare dalla preventiva predisposizione del materiale da sottoporre allo stesso, non tanto al fine di farsi sottoscrivere un foglio di carta per un'eventuale esclusione di responsabilità, ma perché la consapevolezza che si sta lavorando basandosi su una proprietà altrui che viene conferita al professionista, sia esso titolare o responsabile del trattamento, per l'espletamento di un mandato, e che quindi **l'interessato avrà il pieno diritto di conoscere e controllare tipologia, esiti e finalità del trattamento.**

1.

Sintesi schematica del quadro normativo di riferimento

(Dott. Giuseppe Miceli)

1.1 Il quadro normativo in materia di protezione dei dati personali.

In tutti gli Stati membri dell'Unione europea, già a partire dal 25/05/2018[2], si applica il Regolamento UE 2016/679 *"relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati"* (in inglese *General Data Protection Regulation*, più noto con l'acronimo G.D.P.R.) il quale ha abrogato la Direttiva 95/46/CE[3].

STRUTTURA DEL GDPR	
Considerando	**173**
Capo I **disposizioni generali**	Art. 1 oggetto e finalità Art. 2 ambito di applicazione materiale Art. 3 ambito di applicazione territoriale Art. 4 definizioni
Capo II – Principi	
Capo III	Sezione 1 – trasparenza e modalità

[2]Il Regolamento UE 2016/679 (cosiddetto G.D.P.R., acronimo di *General Data Protection Regulation*) del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE è stato pubblicato il 4 maggio 2016 sulla Gazzetta Ufficiale dell'Unione Europea. Al fine di agevolare l'adeguamento degli ordinamenti giuridici dei singoli Paesi membri il legislatore comunitario ha previsto un periodo di *vacatio* della durata di 2 anni, durante il quale il GDPR pur essendo vigente non poteva ancora considerarsi applicabile. La piena applicabilità del GDPR è scattata, dunque, alla scadenza del biennio di *vacatio*, ovvero: il 25 maggio 2018.

[3]Il quadro normativo UE in materia di protezione dei dati personali si fonda sul *General Data Protection Regulation* (che consta di 99 articoli e 173 "considerando") e sulla Direttiva (UE) n. 2016/680 che disciplina i trattamenti effettuati dalle autorità competenti, a fini di: prevenzione, indagine, accertamento e perseguimento di reati; esecuzione di sanzioni penali e salvaguardia e prevenzione di minacce alla sicurezza pubblica; risulta invece definitivamente abrogata la n. 95/46/CE.

diritti dell'interessato	Sezione 2 – Informazione e accesso ai dati personali Sezione 3 – rettifica e cancellazione Sezione 4 – diritto di opposizione e processo decisionale automatizzato relativo alle persone fisiche Sezione 5 – limitazioni
Capo IV **titolare del trattamento e responsabile del trattamento**	Sezione 1 – obblighi generali Sezione 2 – sicurezza dei dati personali Sezione 3 – valutazione d'impatto sulla protezione dei dati e consultazione preventiva Sezione 4 – responsabile della protezione dei dati Sezione 5 – codici di condotta e certificazioni
Capo V **trasferimento di dati personali verso paesi terzi o organizzazioni internazionali**	
Capo VI **autorità di controllo indipendenti**	Sezione 1 – Indipendenza Sezione 2 – Competenza, compiti e poteri
Capo VII **Cooperazione e coerenza**	Sezione 1 – Cooperazione Sezione 2 – coerenza Sezione 3 – comitato europeo per la protezione dei dati
Capo VIII **mezzi di ricorso, responsabilità e sanzioni**	
Capo IX **disposizioni relative a specifiche situazioni di trattamento**	
Capo X **atti delegati e atti di esecuzione**	
Capo XI	

disposizioni finali	

GEOGRAFIA DEL GDPR	
Artt. 2-4	**Ambito di applicazione del Regolamento**
Artt. 5-10	**Principi applicabili al trattamento dei dati personali**
Artt. 12-21	**Diritti dell'interessato**
Artt. 4; 24; 26-29; 37-39	**Figure e ruoli**
• Art. 28, commi 3, 4 • Artt. 32, 33 • Artt. 24, 25, 30 • Artt. 35-36; 40-43	**Obblighi generali** • Gestione dei responsabili del trattamento • Sicurezza dei dati personali • *Accountability, Privacy by design*, Registro delle attività di trattamento • DPIA, Consultazione preventiva, Codici di condotta, Certificazioni
Artt. 44-49	**Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali**
Artt. 51; 52; 55-58; 60-62; 64; 68-76	**Autorità di controllo e Comitato Europeo per la Protezione dei Dati**
Artt. 77-79; 82-84	**Mezzi di ricorso, responsabilità e sanzioni**

Il GDPR introduce nell'ambito delle attività che si definiscono *"trattamento dei dati personali"* una serie di rilevanti novità, improntate al valore della *"cultura della privacy"* e con effetto obbligatorio, che possono essere schematizzate nella seguente tabella riepilogativa.

PRINCIPALI NOVITÀ PREVISTE DAL GDPR	
Rif.	**Descrizione**
C. II – Art. 5	Il trattamento dei dati deve essere effettuato in modo lecito, corretto e trasparente nel rispetto dell'interessato. Il trattamento deve indicare le finalità che lo giustificano. Tali finalità devono essere determinate, esplicite e legittime. Inoltre, i dati oggetto del trattamento devono essere raccolti rispettando criteri di: adeguatezza, pertinenza, esattezza e devono essere aggiornati e coerenti con la dichiarata finalità, in ogni caso trattati in maniera tale da poterne "comprovare" un'adeguata sicurezza.
C. II –	Il titolare del trattamento è obbligato ad acquisire il consenso del soggetto interessato,

Artt. 6, 7	salvo il caso in cui sia espressamente previsto l'esonero dalla richiesta. Il titolare deve essere in grado di "comprovare" che tale consenso sia stato effettivamente prestato e che lo stesso si basi su una comunicazione espressa: in forma comprensibile e facilmente accessibile; formulata con un linguaggio semplice e chiaro.
C. II – Art. 8	In relazione al trattamento di dati relativi all'offerta diretta di servizi della società dell'informazione verso i minori, vi è liceità se il minore che ha prestato il consenso abbia compiuto 16 anni. Se il minore non abbia ancora compiuto i 16 anni (ma ne abbia compiuti almeno 13) è necessario acquisire il consenso di chi ne esercita la responsabilità genitoriale. Spetta al titolare del trattamento la responsabilità, in considerazione delle tecnologie disponibili, di verificare tale circostanza relativa all'età. (il D.Lgs 101/2018 ha abbassato la soglia di età da 16 ad anni 14).
C. II – Art. 9	Divieto generale del trattamento dei dati corrispondenti a quelli che il Codice della privacy definiva 'sensibili' e ora "particolari". Sono previste eccezioni a tale divieto nelle ipotesi in cui: l'interessato abbia espresso il consenso; i dati siano trattati per l'esecuzione di un contratto di lavoro nonchè per assicurare l'adempimento degli obblighi in materia di sicurezza/protezione sociale.
C. II – Art. 10	Il trattamento dei dati personali 'giudiziari' richiede, alternativamente, il controllo della Autorità pubblica o la preventiva autorizzazione in virtù di norme dell'Unione e del singolo Stato membro che prevedano garanzie appropriate per i diritti e le libertà degli interessati.
C. III – Art. 12	Il titolare ha l'obbligo di adottare le misure idonee a fornire all'interessato tutte le informazioni/comunicazioni relative ai trattamenti dallo stesso effettuati, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. Il titolare, deve agevolare l'esercizio dei diritti da parte dell'interessato e deve fornire risposta a tutte le richieste dell'interessato, senza ingiustificato ritardo e comunque entro 30 giorni dal ricevimento della richiesta stessa (termine è prorogabile fino a 60 giorni, in considerazione della complessità e del numero delle richieste).
C. III – Artt. 13, 14	Il Titolare del trattamento è obbligato a rendere l'informativa all'interessato. L'informativa deve rispettare una serie di criteri: il titolare del trattamento deve indicare espressamente il periodo di conservazione dei dati personali, i criteri utilizzati per determinare tale durata, utilizzando un linguaggio espositivo semplice e chiaro. Il GDPR distingue i casi in cui la comunicazione delle informazioni sia collegata alla raccolta dei dati avvenuta presso l'interessato (art. 13) da quella che presuppone la raccolta ei dati effettuata presso un soggetto diverso (art. 14).
C. III – Artt. 15, 16, 17, 18, 20, 21	Si estende il catalogo di diritti dell'interessato: il diritto di accesso, il diritto di rettifica, il diritto alla cancellazione (cd diritto all'oblio), il diritto di limitazione del trattamento, il diritto alla portabilità dei dati, il diritto di opposizione al trattamento e i corrispondenti diritto di ricevere dal titolare notifica/comunicazione di eventuale violazione dei dati personali (*Data breach*).
C. III – Art. 22	Diritto dell'interessato a non essere sottoposto a una decisione basata esclusivamente su un trattamento automatizzato dei dati (profilazione) che produca effetti giuridici che lo riguardano o che possa incidere significativamente sulla sua persona. Il divieto trova limite nell'esplicito consenso fornito dall'interessato, nella necessità ai fini dell'esecuzione di un contratto con l'interessato, ovvero nei casi autorizzati dal diritto dell'Unione o del singolo Stato membro.
C. IV –	Il titolare del trattamento deve adottare misure tecniche e organizzative adeguate al fine

Artt. 24, 32	di garantire, ed essere in grado di "comprovare" la conformità del trattamento, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche. Le misure devono essere sottoposte a un periodico riesame e aggiornamento.
C. IV – Art. 25.1	La *Privacy by design* (ovvero, fin dalla progettazione) Principio di *privacy by design*: il titolare del trattamento, in considerazione delle specifiche caratteristiche del trattamento nonché degli specifici profili di rischio verso i diritti e le libertà delle persone fisiche (soggetti interessati), è obbligato a determinare e adottare misure tecniche e organizzative adeguate, finalizzate ad attuare efficacemente i principi di protezione dei dati e garantire che il trattamento sia conforme ai requisiti sanciti dal Regolamento per la tutela dei diritti degli interessati.
C. IV – Art. 25.2	Principio della *privacy by default:* il titolare del trattamento ha l'obbligo di mettere in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ciascuna finalità del trattamento. L'obbligo è commisurato alla quantità dei dati raccolti, alla portata del trattamento, al periodo di conservazione nonché all'accessibilità ai dati stessi.
C. IV – Art. 26	Contitolarità del trattamento dei dati personali che si configura nel caso di due o più titolari che operano nello stesso trattamento (determinando congiuntamente finalità e mezzi del medesimo), concordando in maniera trasparente, sulla base di formale accordo, la ripartizione delle responsabilità del trattamento, con particolare attenzione all'esercizio dei diritti degli interessati e ai connessi obblighi informativi. È obbligatorio mettere a disposizione degli interessati l'accordo di contitolarità.
C. IV – Art. 27	Per il trattamento di dati personali operato da parte di titolare/responsabile quale soggetto non stabilito nell'UE, l'art. 3.2 GDPR statuisce che il titolare/responsabile deve designare - per iscritto - un proprio rappresentante nell'Unione. Il rappresentante si interfaccia con la competente autorità di controllo e gli interessati, in ordine a tutte le questioni riguardanti il trattamento.
C. IV – Art. 28	Il titolare del trattamento nomina il responsabile del trattamento, il quale dovrà essere un soggetto/organismo che presenti garanzie sufficienti per mettere in atto le prescritte misure tecniche e organizzative adeguate.
C. IV – Art. 29	Il titolare del trattamento deve istruire e formare i soggetti da lui autorizzati ad accedere ai dati personali oggetto dei trattamenti che si svolgono nella sua organizzazione, compresi coloro che svolgono il ruolo di responsabile del trattamento.
C. IV – Art. 30	Il titolare del trattamento con almeno 250 dipendenti o che, pur contando meno di 250 dipendenti, effettui un trattamento che possa presentare un rischio per i diritti e le libertà degli interessati che non sia occasionale o che includa dati sensibili, genetici, biometrici, giudiziari è obbligato a tenere il Registro dei trattamenti. Stesso obbligo incombe sul responsabile del trattamento. L'art. 30 del GDPR statuisce quelle che sono le informazioni minime necessarie e che non possono mancare all'interno del registro: – il nome e i dati di contatto del titolare del trattamento, nonché del contitolare, del rappresentante del trattamento e dei suoi responsabili, lo stesso vale per il registro del responsabile;

	– le finalità del trattamento; – descrizione delle categorie di interessati e delle categorie di dati personali; – categorie di destinatari a cui i dati personal sono stati o saranno comunicati, compresi i destinatari dei paesi terzi o di organizzazioni internazionali; – i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale…; – ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati; – ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.
C. IV – Art. 31	Il titolare è tenuto a cooperare con l'Autorità di controllo.
C. IV – Art. 33	Obbligo di notificazione di una violazione dei dati all'autorità di controllo (cioè, il Garante) senza ingiustificato ritardo – e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza - di ogni violazione della sicurezza dei dati personali (*Data breach*) che presenti un rischio per i diritti e le libertà delle persone fisiche.
C. IV – Art. 34	Se a causa della violazione dei dati si configura l'ipotesi di rischio elevato per i diritti e le libertà delle persone fisiche, il titolare ha l'obbligo di darne notizia all'interessato senza ingiustificato ritardo. Il contenuto minimo della comunicazione: linguaggio semplice e chiaro.
C. IV – Artt. 35, 36	Obbligo per il titolare del trattamento di redigere il Documento di Valutazione d'impatto sulla protezione dei dati (DPIA). Il titolare potrà consultare l'autorità di controllo.
C. IV – Artt. 37-39	Nomina obbligatoria del Responsabile della Protezione dei Dati (Data Protection Officer – DPO) nei casi i cui il titolare del trattamento sia: a) autorità/organismo pubblico (eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali); b) effettui trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; c) effettui come attività principali trattamenti su larga scala di dati sensibili, genetici, biometrici, giudiziari. Il DPO (o, in italiano, RPD) ha compiti di informazione, formazione, consulenza e sorveglianza dell'adempimento della disciplina 'privacy'. E' anche interfaccia verso l'Autorità Garante per la privacy. L'art. 37 stabilisce che *"Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39".* L''art. 39 sancisce che: "Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti: a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente Regolamento nonché da altre disposizioni dell'Unione o degli Stati

	membri relative alla protezione dei dati; b) sorvegliare l'osservanza del presente Regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo; c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35; d) cooperare con l'autorità di controllo; e e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione".
C. IV – Artt. 40-42	L'adesione a codici di condotta/sistemi di certificazione. Adempimenti volontari per il titolare che potrà implementare le misure di sicurezza dei trattamenti e dimostrare la conformità delle attività di trattamento ai requisiti stabiliti dal GDPR.
C. V – Artt. 44, 45, 46,47, 48, 49	Il trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale deve essere effettuato nel rispetto di specifiche condizioni affinché non sia pregiudicato il livello di protezione delle persone fisiche.
C. VIII – Art. 82	Il titolare è obbligato a risarcire il danno materiale o immateriale cagionato da una violazione del Regolamento. Lo stesso titolare è esonerato da tale responsabilità nel caso in cui riuscisse a dimostrare che l'evento dannoso non possa essere in alcun modo a lui stesso imputabile.

Il legislatore nazionale, al fine di adeguare l'impianto normativo interno al menzionato Regolamento, ha emanato il D.Lgs. 101/2018[4] che è entrato in vigore il 19 settembre 2018, modificando radicalmente il D. Lgs. n. 196/2003[5], c.d. *Codice della privacy*[6].

Il D.lgs. n.101 del 10.8.18 mostra, tuttavia, alcuni segnali di continuità rispetto al precedente testo del *Codice della privacy* e – coerentemente con quanto sancito dal legislatore comunitario[7] – "tiene in vita"

[4] Decreto Legislativo 10 agosto 2018, n. 101 *Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)*. Pubblicato in GU Serie Generale n.205 del 04-09-2018, entrato in vigore il 19/09/2018.

[5] D. Lgs. 30 giugno 2003, n. 196, «Codice in materia di protezione dei dati personali».

[6] Costituisce addendum al presente volume il Codice privacy emendato.

- seppur per un periodo transitorio - i provvedimenti del Garante e le autorizzazioni, che sono – nel frattempo - oggetto di revisione, come pure i Codici deontologici vigenti che si riferiscono alle differenti categorie professionali.

Il D.Lgs. n. 101 del 10.8.18 - suddiviso in sei Capi e si compone di 27 articoli - ha sancito le seguenti abrogazioni al decreto legislativo n. 196 del 2003, di seguito elencati:	
Parte I -	1) gli articoli 3, 4, 5 e 6; 2) il titolo II, il titolo III, il titolo IV, il titolo V, il titolo VI e il titolo VII;
Parte II -	1) il capo I del titolo I; 2) i capi III, IV e V del titolo IV; 3) gli articoli 76, 81, 83 e 84; 4) il capo III del titolo V; 5) gli articoli 87, 88 e 89; 6) il capo V del titolo V; 7) gli articoli 91, 94, 95, 98, 112, 117, 118 e 119; 8) i capi II e III del titolo X, il titolo XI e il titolo XIII;
Parte III -	1) la sezione III del capo I del titolo I; 2) gli articoli 161, 162, 162-bis, 162-ter, 163, 164, 164-bis,165 e 169; 3) gli articoli 173, 174, 175, commi 1 e 2, 176, 177, 178 e 179; 4) il capo II del titolo IV; 5) gli articoli 184 e 185;
Allegati	B e C.

Di seguito viene riportata la struttura del D Lgs. n. 196/2003, c.d. *Codice della privacy*, così come modificato dal D.Lgs. 101/2018.

[7] Cfr.: art.. 22 (Altre disposizioni transitorie e finali) "1. Il presente decreto e le disposizioni dell'ordinamento nazionale si interpretano e si applicano alla luce della disciplina dell'Unione europea in materia di protezione dei dati personali e assicurano la libera circolazione dei dati personali tra Stati membri ai sensi dell'articolo 1, paragrafo 3, del Regolamento (UE) 2016/679".

STRUTTURA DEL CODICE PRIVACY	
Prefazione	
Parte I	• Titolo I: Principi e disposizioni generali - Art. 1-6 • Titolo II: Diritti dell'interessato (abrogato) - Art. 7-10 • Titolo III: Regole generali per il trattamento dei dati (abrogato) - Art. 11-27 • Titolo IV: Soggetti che effettuano il trattamento (abrogato) - Art. 28-30 • Titolo V: Sicurezza dei dati e dei sistemi (abrogato) - Art. 31-36 • Titolo VI: Adempimenti (abrogato) - Art. 37-41 • Titolo VII: Trasferimento dei dati all'estero (abrogato) - Art. 42-45
Parte II	• Titolo 0.I: Disposizioni sulla base giuridica - Art. 45-bis • Titolo I: Trattamenti in ambito giudiziario - Art. 46-52 • Titolo II: Trattamenti da parte di forze di polizia (abrogato) - Art. 53-57 • Titolo III: Difesa e sicurezza dello Stato - Art. 58 • Titolo IV: Trattamenti in ambito pubblico - Art. 59-74 • Titolo V: Trattamento di dati personali in ambito sanitario - Art. 75-94 • Titolo VI: Istruzione - Art. 95-96 • Titolo VII: Trattamenti a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici - Art. 97-110-bis • Titolo VIII: Trattamenti nell'ambito del rapporto di lavoro - Art. 111-116 • Altri trattamenti in ambito pubblico o di interesse pubblico - Art. 117-120 • Titolo X: Comunicazioni elettroniche - Art. 121-

	134 • Titolo XI: Libere professioni e investigazione privata (abrogato) - Art. 135 • Titolo XII: Giornalismo, libertà di informazione e di espressione - Art. 136-139 • Titolo XIII: Marketing diretto (abrogato) - Art. 140
Parte III	• Titolo I: Tutela amministrativa e giurisdizionale - Art. 140-bis-152 • Titolo II: Autorità di controllo indipendente - Art. 153-160-bis • Titolo III: Sanzioni - Art. 161-172 • Titolo IV: Disposizioni modificative, abrogative, transitorie e finali - Art. 173-
Conclusione	

ELENCO DEI PRINCIPALI PROVVEDIMENTI DEL GARANTE PRIVACY:
• Provvedimento Videosorveglianza (8 aprile 2010)
• Amministratore di Sistema (27 novembre 2008)
• Biometria e firma grafometrica (21 maggio 2014)
• Cookies (8 maggio 2014)
• Posta elettronica e Internet (10 marzo 2007)
• Persone Giuridiche (20 settembre 2012)
• Spam e-mail commerciali (4 luglio 2013)

1.2 Il "dato personale" ai sensi del GDPR: definizione e tipologie di dati

Il GDPR rappresenta lo strumento normativo in grado di ridisegnare i confini di una tutela dei dati personali dei cittadini Ue che sono, evidentemente, sempre più esposti ai rischi di un controllo massivo e dettato – troppo spesso – da logiche commerciali ai limiti della correttezza[8].

Il Regolamento, dunque, consente ai **cittadini UE** di poter esercitare un maggiore e **più effettivo controllo sui propri dati personali**. Ecco quindi che assume un valore dirimente individuare la corretta definizione di ciò che il legislatore comunitario considera essere "dato personale". A ben vedere, la classificazione dei dati personali contenuta nell'art. 4 del GDPR non si discosta dalla precedente definizione, ovvero da quella che il legislatore nazionale aveva delineato nell'art. 4 del D. Leg.vo n. 196/2003, tuttavia, la nuova formulazione denota l'esigenza di **adeguare la definizione di "dato personale" all'attuale contesto sociale ed economico**, fortemente influenzato dal continuo progresso tecnologico.

Secondo il GDPR, i dati personali sono "*qualsiasi informazione*" che riguarda "*una persona fisica identificata o identificabile*"[9]. Dato personale è, pertanto, "*qualsiasi informazione riguardante una persona fisica almeno identificabile*"[10].

ELEMENTI SU CUI SI FONDA LA DEFINIZIONE DI "DATO PERSONALE"	
Persona fisica	Il diritto alla protezione dei dati è riconosciuto nell'ambito del diritto alla libertà e alla vita privata
"qualsiasi informazione"	Tutte le informazioni sono rilevanti e possono ricadere nell'area di applicazione dell'art. 4 GDPR, a prescindere da giudizi di rilevanza *ex ante*. Il legislatore indica un elenco esemplificativo e non esaustivo di "dati personali" che comprende: *"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"*.
	Contenuto informativo che consente il collegamento funzionale ovvero l'identificazione della persona fisica, anche solo indirettamente e anche solo in termini probabilistici.

[8] Il GDPR si applica ai soggetti/imprese che abbiano sede in territorio UE, nonché a quelli che pur avendo sede al di fuori dall'Unione europea, trattano dati personali relativi a cittadini UE o, ancora, che svolgano attività di monitoraggio del comportamento di soggetti localizzati nell'UE.

[9] Così: Regolamento UE 2016/679, Art.4 – Definizioni.

[10] *Ibidem*.

Identificazione/Identificabilità	
Ragionevole probabilità	Si tratta di *"qualsiasi processo anche meramente deduttivo, attraverso il quale è possibile approdare all'identificazione"*[11]. La ragionevole probabilità è collegata a parametri oggettivi, cioè fattori previsti dalla legge come, per esempio, le tecnologie disponibili al momento del trattamento.

La nozione di dato personale si fonda su quattro fattori:

CLASSIFICAZIONE DI "DATI PERSONALI" AI SENSI DELL'ART. 4 GDPR	
TIPOLOGIA DI DATO	**COSA PREVEDE IL GDPR**
Dato personale	"qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale"
Dati genetici	"i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione"
Dati biometrici	"i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici"
Dati relativi alla salute	"i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute"
"CATEGORIE PARTICOLARI DI DATI PERSONALI"AI SENSI DELL'ART. 9 GDPR	
Dati particolari	dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

[11] Cfr.: Bistolfi C., Bolognini L., Pelino E., *Il Regolamento Privacy europeo, Commentario alla nuova disciplina sulla protezione dei dati personali*, Giuffrè, 2016.

"CATEGORIE PARTICOLARI DI DATI PERSONALI"AI SENSI DELL'ART. 10 GDPR	
Dati giudiziari	Informazioni relative a reati o condanne penali e a connesse misure di sicurezza. Il trattamento di tali dati richiede il controllo dell'autorità pubblica (art. 10 GDPR)[12]. Si pensi che la tenuta del "casellario giudiziale" può essere affidata esclusivamente al controllo dell'autorità pubblica.
Art. 22, c. 2, D.Lgs. 101/2018: «A decorrere dal 25 maggio 2018 le espressioni "dati sensibili" e "dati giudiziari" utilizzate ai sensi dell'articolo 4, comma 1, lettere d) ed e), del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, ovunque ricorrano, si intendono riferite, rispettivamente, alle categorie particolari di dati di cui all'articolo 9 del Regolamento (UE) 2016/679 e ai dati di cui all'articolo 10 del medesimo Regolamento. A decorrere dal 25 maggio 2018 le espressioni "dati sensibili" e "dati giudiziari" utilizzate ai sensi dell'articolo 4, comma 1, lettere d) ed e), del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, ovunque ricorrano, si intendono riferite, rispettivamente, alle categorie particolari di dati di cui all'articolo 9 del Regolamento (UE) 2016/679 e ai dati di cui all'articolo 10 del medesimo Regolamento».	

[12] Il trattamento di dati personali effettuato da autorità pubblica di sicurezza ai fini della prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, non è disciplinato dal GDPR ma dalla Direttiva EU 2016/680.

2.

Organigramma privacy: ruoli e responsabilità

(Avv. Luca Malatesta)

2.1 Situazioni di titolarità e contitolarità del trattamento: come distinguerle e cosa fare

Con buona pace di tutti coloro che hanno in passato svolto tentativi di ancorare un'analisi dei rischi al dato dimensionale delle realtà indagate, **nel Regolamento non c'è alcuna traccia di riferimenti alla dimensione aziendale**. Nel mondo degli studi professionali quanto sopra comporta che chi si appresta a gestire il rischio privacy, immediatamente dopo aver analizzato i trattamenti posti in essere all'interno dello studio, dovrà mappare l'organigramma dello stesso avendo riguardo a istruzioni e garanzie precise, chieste e date, nell'ambito dei trattamenti dei dati svolti. Infatti, qualunque studio professionale, anche il più piccolo, vede comunque una circolazione dei dati cointeressare una pluralità **di responsabili** che dovranno essere incaricati, controllati e supervisionati dal titolare del trattamento.

L'approccio metodologico che - a parere di chi scrive - è quello sicuramente più proficuo per poter determinare l'ampiezza del raggio d'azione dei singoli poteri del responsabile del trattamento e conseguente garanzie e responsabilità dello stesso, ci viene offerto dalla **nozione di consenso** individuata nel Regolamento. La dialettica tra il diritto a un consenso al trattamento che sia **libero, specifico e non estorto in alcun modo,** riconosciuto all'interessato dagli articoli 6 e 7 del Regolamento, e il correlativo diritto del titolare a portare avanti il trattamento in conformità alla base giuridica dello stesso, trova peculiare applicazione **nella realtà dello studio professionale, dove il rapporto contrattuale ha fortissime connotazioni fiduciarie**, potendo arrivare a dire che nella maggior parte dei rapporti tra professionista e cliente, il rapporto dura finché dura la fiducia.

Orbene, potendo identificare il consenso come *"qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di*

trattamento"[13] ne consegue che il consenso raccolto dal professionista nell'ambito del proprio mandato porti a far coincidere il titolare del trattamento con il professionista investito dell'incarico, anche all'interno - ad esempio - di una sola struttura associata. Difatti, dovendo tracciare l'organigramma privacy di una struttura tipicamente medio-piccola come uno studio professionale[14], un approccio tipicamente utile è quello di seguire il consenso prestato al professionista al momento del conferimento dell'incarico per individuare il titolare. Ne consegue, altrettanto automaticamente, che di contitolarità all'interno dello studio, si potrà parlare solo quando l'incarico verrà congiuntamente affidato a due professionisti, come a esempio nel caso di due avvocati che difendono il medesimo imputato all'interno dello stesso processo penale. In tale situazione, avendo riguardo alla riservatezza dei dati sensibili giudiziari del loro assistito, ognuno dei due difensori sarà responsabile della propria condotta, ma anche di un obbligo rafforzato di vigilanza sulla condotta del collega per evitare rischi per la riservatezza.

Difficilissimo anche immaginare una situazione di contitolarità tra un soggetto professionista che riceva un mandato (tipicamente fondato sulla fiducia, cfr. l'articolo 35 del Codice deontologico Forense), e un soggetto imprenditore che riceva un mandato contestuale[15].

La situazione differente in cui un singolo professionista riceva il mandato e deleghi le attività di gestione del procedimento a un collega, invece, configura un ordinario rapporto titolare - responsabile, di cui si tratterà nel prosieguo.

L'approccio di parametrare la definizione di un **rapporto tra più soggetti che gestiscono il dato sensibile come titolare - responsabile oppure contitolare** del trattamento, tenendo conto delle peculiarità delle prerogative di legge riservate alle professioni ordinistiche, trova conforto nel provvedimento con cui il Garante ha risposto ai quesiti del Consiglio Nazionale dei Consulenti del Lavoro[16] in base alla lettura testuale dell'art. 7 del GDPR che definisce " "*«titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali"*, chiedevano la qualificazione del professionista come titolare o contitolare del trattamento. Orbene, nella decisione del Garante il

[13]Questa è la definizione data dal Regolamento all'articolo 4.11.

[14]D'all'ultimo censimento ISTAT 2011 risulta che su 748 ben 656 studi professionali regolamentati e 739 contavano da zero a nove addetti.

[15]Basti pensare alla situazione, diffusissima nella pratica, in cui un imprenditore conferisca mandato professionale ad un dottore commercialista e contestualmente, un contratto di servizi con un centro elaborazione dati per tutte le attività non riservate dalla legge ai professionisti regolamentati.

[16]Per la consultazione della risposta del Garante privacy al quesito formulato dal Consiglio Nazionale dei Consulenti del Lavoro: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9080970

consulente del lavoro è inquadrato come responsabile del trattamento in quanto riceve (ovviamente su base lecita) i dati raccolti dal titolare - cliente, ossia il datore di lavoro nell'ambito delle sue prerogative in base ad un mandato sottoscritto in conformità alle leggi vigenti.

A sommesso parere di chi scrive, la centralità attribuita dal Regolamento alla figura dell'interessato che gestisce tramite il consenso (concedendolo, modificandolo, o regolandolo), dovrebbe imporre all'interprete di utilizzare questo fondamentale parametro nell'ambito dell'attività ermeneutica quando si accosta alla prima, fondamentale operazione di mappatura di soggetti e funzioni. Una sorta di ricerca a ritroso che partendo dal consenso liberamente concesso dall'interessato, qualifica il titolare e, a cascata, i responsabili a cui il titolare impartisce istruzioni e chiede garanzie.

A ben vedere, utilizzando tale approccio, **due avvocati che ricevono il mandato congiunto a difendere un imputato saranno contitolari,** il consulente del lavoro responsabile del trattamento dei dati raccolti dal datore di lavoro, **un commercialista e il CED titolari autonomi** quando il cliente sottoscriva due separati contratti (mandato fiduciario al professionista, contratto di servizi con l'azienda), ovvero titolare e responsabile qualora nel contratto di mandato del professionista sia menzionato il ricorso all'attività del centro di elaborazione dati.

Medesimo discorso vale per i sanitari che operino in regime libero professionale (cioè non inquadrati nell'organigramma della struttura sanitaria). Il medico è sempre titolare del trattamento qualora riceva le informazioni (e quindi il consenso) in base ad un rapporto fiduciario dal paziente, anche se all'interno di una struttura alla quale non è legato da un rapporto di lavoro. **Esclusa,** pertanto, **la possibilità di un consenso** (come purtroppo si trovano spesso) **"dello studio professionale"** che a differenza della privacy "di struttura" non è possibile, sarà cura del professionista designare un eventuale struttura, magari individuando anche il personale di segreteria come responsabile del trattamento e vigilare delle garanzie prestate dalla stessa.

2.2 Il responsabile del trattamento

Proseguendo nel tentativo di organizzare i soggetti orbitanti attorno ai dati dell'interessato, dopo aver avuto cura di individuare titolari e contitolari del trattamento, l'operazione generalmente più laboriosa è l'individuazione e la gestione in termini di incarico dei vari responsabili.

Se nello studio professionale il professionista che riceve il mandato coincide invariabilmente con il titolare del trattamento, nella stragrande maggioranza dei casi questa attività viene coadiuvata da altri professionisti, collaboratori, ausiliari, personale di segreteria amministrativa e tecnica, fino ad arrivare a coloro i quali, in virtù di un contratto di fornitura o di servizi, due esempi per tutti informatica e pulizie,

si trovi ad avere accesso a dati o archivi. Essendo il titolare destinatario dei dati che tratta col consenso dell'interessato e di cui determina mezzi e finalità, ed essendo venuta meno la figura dell'incaricato, possiamo inquadrare tutti i soggetti a vario titolo designati dal titolare, dallo stesso incaricati e sottoposti al suo potere di controllo nell'unica categoria dei responsabili del trattamento. In questo modo, senza declinazioni intermedie, **ogni nodo dell'organigramma privacy di uno studio professionale, dovrebbe essere occupato da una figura inquadrata come responsabile** del trattamento, alla quale **dovrà essere impartita un'adeguata formazione,** non solo sul dettato della legge in generale, ma anche sulle modalità specifiche di gestione del dato all'interno della realtà specifica nel singolo studio professionale. Non deve sfuggire, infatti, come all'interno della realtà dello studio professionale, la maggior parte delle attività di consulenza, vigilanza, formazione, produzione documentale, cioè tutte quelle attività che vengono normalmente raggruppate all'interno dei sistemi di gestione per la sicurezza delle informazioni, abbiano come destinatari i vari responsabili del trattamento che a vario titolo "toccano" i dati dell'interessato.

La mappatura dei responsabili diventa così il primo passo per una stringente analisi riguardo all'ampiezza del loro ruolo, al livello di rischio della loro operatività in concreto, alla personalizzazione massima delle mansioni e delle attività specifiche di gestione del dato.

In particolare, giova ricordare che nel rapporto tra titolare e responsabile, il titolare (e questo è ancor più vero proprio nella misura in cui si parli di studi professionali) ha "negoziato" il consenso ricevuto dall'interessato nell'alveo del proprio incarico, delle norme deontologiche di categoria e delle eventuali leggi professionali, mentre **il responsabile è mero esecutore delle direttive del titolare** e non risponde se non per violazione delle stesse. Sarà quindi fondamentale da parte del titolare innanzitutto presentare ai responsabili lettere di incarico, regolamenti, istruzioni che siano stringenti, chiare e soprattutto evitino di assomigliare a dei prestampati uguali per tutti.

Altra cura fondamentale andrà prestata al livello culturale del responsabile: se lo studio annovera tra il personale di segreteria soggetti con alfabetizzazione informatica quasi nulla, un incarico che contenga la prescrizione a dotarsi di password che abbiano un algoritmo di cifratura con chiave a 64 *bit*, potrebbe essere - mi si passi l'espressione calcistica - un clamoroso *autogol* qualora ci si dovesse difendere da contestazioni.

2.3 La categoria dei sub-responsabili del Titolare o del Responsabile per il trattamento

Nuova figura espressamente menzionata nell'articolo 28 del Regolamento, i **sub-responsabili** del trattamento sono quei soggetti che possono essere nominati responsabili del

trattamento. Infatti l'articolo menzionato, al secondo comma stabilisce che il responsabile del trattamento non ricorre a un altro responsabile senza previa **autorizzazione scritta, specifica o generale,** del titolare del trattamento.

Nel caso di autorizzazione scritta, in generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche. Il comma preso in esame risolve molti dei problemi applicativi, soprattutto in realtà complesse, laddove catene di appalto subappalto che comportano trattamento dei dati sono all'ordine del giorno, si pensi ad esempio a settori come l'informatica o il credito. In realtà, negli studi professionali, proprio in virtù delle dimensioni generalmente piuttosto contenute delle realtà del settore, è difficile imbattersi in lunghe catene di sub-responsabili.

Anche nell'ipotesi abbastanza residuale di un medico generico libero professionista che chieda un consulto lo specialista libero professionista che a sua volta si avvalga di altro specialista, al medico generico titolare del trattamento verrà comunque data la possibilità di interfacciarsi direttamente con il secondo specialista nominandolo responsabile del trattamento in modo diretto.

Medesimo discorso potrà farsi ad esempio con gli ausiliari dell'avvocato come un consulente medico di parte il quale verrà addirittura investito di autonomo consenso al trattamento dei dati da parte dell'interessato diventando a sua volta titolare del trattamento.

Un settore professionale, invece, in cui il secondo comma dell'articolo 28 del Regolamento è di particolare attualità, è quello dei consulenti del lavoro, oppure dei commercialisti, categorie che fanno ricorso in modo massiccio all'utilizzo di software gestionali che prevedono attività di *data entry* anche di dati sensibili su database gestiti da grandi aziende di informatica, che hanno loro volta dietro reti di sub-responsabili. In questo caso il sub-responsabile, secondo quanto disposto dal Regolamento, è tenuto a rispettare i medesimi obblighi contrattuali che legano il titolare al primo responsabile, prevedendo in particolare garanzie sufficienti e la messa in atto di misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento.

Con riguardo alla **responsabilità, a** rispondere davanti al titolare di eventuali inadempienze del sub-responsabile sarà il responsabile direttamente incaricato dal titolare, anche ai fini del risarcimento, fatta salva ovviamente la possibilità di dimostrare che l'evento dannoso non gli è in alcun modo imputabile[17].

[17] Cfr. Art. 82 pp 1-3 GDPR.

Questo tipo di gestione della responsabilità vale ovviamente sia per i professionisti regolamentati in generale, ma anche per i consulenti del lavoro che, come infra analizzato, essendo stati incaricati non dall'interessato ma dal datore di lavoro titolare del trattamento si trovano a essere responsabili e quindi ad avere attorno quali ausiliari soltanto sub-responsabili.

2.4 Il DPO Data Protection Officer

La figura del ***Data Protection Officer*** (definizione a parere di chi scrive preferibile alla traduzione italiana responsabile della protezione dei dati, poiché enfatizza il ruolo di garanzia e l'indipendenza del DPO), potrebbe sembrare a tutta prima di scarsa importanza in una trattazione relativa alla realtà dello studio professionale. Al contrario, è proprio nelle professioni regolamentate e negli attributi tipici di indipendenza del professionista che il *munus*[18] del *Data Protection Officer* si estrinseca compiutamente. Sin dalla scelta terminologica del termine *officer*, che negli ordinamenti di *Common law* è generalmente riferito a una figura che sia pubblico ufficiale o incaricato di un pubblico servizio, il legislatore ha posto l'accento sulla **funzione di garanzia** e quindi nella **correlativa necessaria indipendenza**, che il DPO ha nei confronti della platea degli interessati in particolare e del singolo interessato che abbia a esercitare.

Prima ancora di definire i compiti del DPO all'art. 39, già in quello precedente si statuisce l'obbligo di fornire i dati di contatto dello stesso agli interessati in maniera indifferenziata, affinché gli stessi possano *"contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente Regolamento"*. Ulteriori punti di contatto tra la figura in esame ed il professionista regolamentato sono la sottoposizione dello stesso *ex lege* al **segreto** e all'obbligo di riservatezza, ma soprattutto la remissione da parte di un eventuale datore di lavoro del proprio potere datoriale, tanto sotto il profilo potestativo che in quello sanzionatorio, per i compiti specifici afferenti la carica (non le mansioni, appunto), conferita. **Lo studio professionale, con l'eccezione probabilmente delle più grandi realtà** associate, resta **fuori dai casi in cui la nomina di un *Data Protection Officer* sia adempimento obbligatorio**: anche l'ipotesi di effettuare come attività principale il trattamento su larga scala di dati sensibili, genetici, biometrici e giudiziari, di cui all'articolo 37, comma 1 *punto c* del Regolamento, lascia fuori dall'obbligo la massima parte degli studi professionali[19].

[18] la funzione

[19] Un discorso a parte riguarda gli studi consulenza del lavoro.

Tutt'altro discorso, è ragionare in merito all'opportunità della nomina del DPO, all'interno di uno studio professionale associato in cui le situazioni di titolarità simultanea sul medesimo cliente da parte di più professionisti siano frequenti e interferenti tra di loro.

Nella logica di gestione della titolarità del trattamento in base al consenso e al mandato fiduciario**, il professionista regolamentato che riceva l'incarico direttamente dall'interessato è titolare, altrimenti è responsabile** se svolge la propria prestazione d'opera intellettuale per un titolare del trattamento che ha già ricevuto il consenso da parte dell'interessato[20].

Ne consegue che immaginare **in una situazione di studio associato, ancor più se multidisciplinare** una "privacy di struttura" in modo analogo a come accade nelle realtà d'impresa sia piuttosto arduo. Per quanto la cosa possa essere risolta attraverso la stesura di appositi regolamenti**, l'esercizio dei diritti dell'interessato potrebbe venire pregiudicato** a una certa confusione, soprattutto in caso di più professionisti separatamente titolari dei trattamenti sullo stesso cliente, si pensi ad esempio ad uno studio medico o addirittura odontoiatrico associato in cui diversi clinici trattino per diversi ambiti lo stesso paziente.

In tal caso valutare l'opportunità di **istituire un *officer* all'interno della realtà associata** per garantire all'interessato un accesso fluido e univoco ai propri dati e ai correlativi diritti potrebbe essere il **miglior modo**, oltre che per raggiungere l'agognata conformità normativa, anche **per snellire notevolmente procedure interne, formazione del personale,** e in generale tutte quelle attività ridondanti che caratterizzano quelle realtà, come gli studi associati in cui un gran numero di attività similari vengono portate avanti da diversi soggetti.

Come accennavo poc'anzi, un discorso a parte in merito all'opportunità della nomina del *Data Protection Officer* riguarda gli **studi di consulenza del lavoro**, soprattutto in forma associata. Questa particolare categoria di professionisti regolamentati ha moli di dati in gestione, in virtù dell'effetto moltiplicativo generato da ogni cliente impresa per i suoi dipendenti, sconosciute alle altre categorie.

Il trattamento su larga scala di dati sensibili e giudiziari, è un elemento che ricorre nella quasi totalità dei casi. I numerosi adempimenti come assunzioni, licenziamenti, gestione degli infortuni sul lavoro, portano il personale degli studi, oltre ai professionisti, ad avere contatto continuo con grandi masse di dati con le modalità più varie. La loro qualifica di responsabili li obbliga, inoltre, a muoversi nell'alveo delle istruzioni ricevute dal titolare del trattamento, che è l'impresa-cliente.

[20] Ad esempio il consulente del lavoro per i dati dei dipendenti dei propri clienti.

Né risulta un quadro di particolare complessità che difficilmente può essere risolto senza la nomina di un professionista o la designazione di un dipendente a ricoprire la qualifica per dirimere quella stessa complessità.

2.5 La gestione degli archivi cartacei e il registro dei trattamenti

2.5.1 La gestione degli archivi cartacei

Quando ci si ponga nell'ottica dell'applicazione del Regolamento europeo alla realtà degli studi professionali, è impossibile non incappare nella, spesso problematica, gestione degli archivi. Tanto dal punto di vista dell'applicazione di misure adeguate per garanzia della sicurezza dei dati - argomento che tratteremo in seguito - quanto perché la nozione di *archivio di dati personali*, che sia esso cartaceo o informatico, decentrato o all'interno di una singola locazione fisica, delimita l'ambito di applicazione materiale del Regolamento in relazione ai trattamenti i dati non automatizzati. **Il concetto di archivio**, di cui all'art. 4 del Regolamento, discendente dalla direttiva 95/46 e altre normative nazionali, non era ripreso **nel nostro Codice Privacy,** che però **non aveva norme di riferimento** che limitassero l'ambito di applicazione rispetto ai trattamenti manuali. Tutte le nozioni di archivio proposte, nella foga del legislatore di fornire criteri che riguardassero il più ampio numero di casi possibili da sottoporre a tutela da parte dell'autorità, ha posto numerosi problemi, interpretativi e pratici. Questo perché, nel momento in cui la nozione di archivio venga interpretata estensivamente (con riferimento a qualunque insieme di dati organizzati), il meccanismo creato dal combinato disposto con la nozione di dato personale contenuta nel Regolamento, finirebbe per configurare obblighi di *accountability* anche della compilazione - scherzo ma non troppo - della lista di amici da invitare al proprio matrimonio.

Già in epoca pre-GDPR le autorità giudiziarie erano intervenute per limitare la nozione di archivio (con riferimento, ad esempio, alla sola tenuta di archivi informatici organizzati per campi) per circoscrivere tale estesissima nozione. Un criterio interpretativo unitario degno di nota lo ha fornito la Corte di Giustizia Europea con la sentenza del 10 luglio 2018, relativa alla direttiva 95/46 ma comunque emessa sotto la vigenza del Regolamento, tant'è che l'Avvocato generale ha fatto riferimento al RRegolamento nella propria opinione che ha preceduto la sentenza.

Nella sentenza si stabilisce quale **criterio determinante** perché un insieme di dati personali possa essere definito archivio, **che lo stesso sia strutturato secondo criteri specifici che consentono di recuperarli facilmente per un successivo impiego**[21].

[21] ARRÊT DE LA COUR (grande chambre) 10 juillet 2018, dans l'affaire C-25/17, «*Renvoi préjudiciel – Protection des personnes physiques à l'égard du traitement des données à caractère personnel – Directive 95/46/CE –Champ d'application de ladite directive – Article 3 – Collecte de données à caractère personnel par les membres d'une*

La responsabilità della tenuta di un archivio si estrinseca, ai sensi del Regolamento, in una gestione che consenta un'agevole esercizio dei diritti dell'interessato innanzitutto, oltre all'adozione di misure tecniche volte a garantire riservatezza ed integrità dei dati. Titolare e responsabile del trattamento, lo si è già visto, sono i soggetti per cui esiste una espressa previsione normativa che li obbliga ad una archiviazione dei dati a loro affidati dagli interessati che si affianca ed aggiunge a tutte le altre previsioni normative per categoria di professionisti regolamentati, come ad esempio quelle relative all'obbligo di conservazione dei documenti fiscali o delle cartelle cliniche, aggiungendo oneri ulteriori proprio in merito alla possibilità che l'interessato, nel pieno esercizio dei suoi diritti, chieda ad esempio copia o cancellazione dei propri documenti. In particolare numerose criticità sotto i profili della privacy si potrebbero rilevare della **delicata fase di un subentro di un professionista sul medesimo mandato**, come **ad esempio la sostituzione del difensore** in corso di causa, allorché, in ossequio alla previsione normativa della portabilità dei dati, venga fatta richiesta della predisposizione della documentazione in vista del passaggio di consegne.

2.5.2 Il registro dei trattamenti

Il registro delle attività di trattamento, previsto dall'articolo 30 del Regolamento Europeo **costituisce uno dei principali elementi di *accountability* del titolare.** In sede di verifica, poi, finisce per essere un vero e proprio biglietto da visita nel delineare un quadro aggiornato dei trattamenti in essere all'interno dell'organizzazione presa in esame, in questo caso lo studio professionale.

Conformemente allo spirito del Regolamento, viene fissata una **soglia di obbligatorietà per la redazione del registro al di sopra dei 250 dipendenti,** prevedendo però altresì l'obbligo per qualunque titolare o responsabile del trattamento che effettui trattamenti che possano presentare rischi, anche non elevati, per i diritti e le libertà delle persone o che effettui trattamenti non occasionali di dati oppure trattamenti di particolari categorie di dati (come ad esempio i dati biometrici, quelli genetici ovvero relativi allo stato di salute, convinzioni religiose, appartenenza politica, origine etnica ecc.), o ancora i dati relativi a condanne penali e reati.

Il Garante per la protezione dei dati personali specifica **l'obbligo di redazione del registro dei trattamenti per tutti i liberi professionisti con almeno un dipendente e/o che trattino dati**

---

communauté religieuse dans le cadre de leur activité de prédication de porte-à-porte – Article 2, sous c) – Notion de "fichier de données à caractère personnel" – Article 2, sous d) – Notion de "responsable du traitement" – Article 10, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne»

sanitari e/o dati relativi a condanne penali e reati ad esempio commercialisti, notai, avvocati, osteopati, fisioterapisti e medici in generale.

Per quanto riguarda i contenuti, il Regolamento Europeo fornisce una individuazione di dettaglio delle informazioni che vanno riportate all'interno del registro delle attività di trattamento, e delle modalità di compilazione per le quali si rimanda tanto alla lettera della legge, quanto alle spiegazioni e ai modelli che l'autorità garante ha messo a disposizione sul proprio sito[22].

Vale la pena, a parere di chi scrive, porre l'accento sull'espressa previsione normativa di **obblighi ulteriori per la creazione del registro dei trattamenti** del responsabile del trattamento.

Come è stato detto sopra, con l'unica notabile eccezione fatta per l'attività di elaborazione paghe da parte dei consulenti del lavoro, il professionista regolamentato all'interno della sua attività "propria" è *sempre* il titolare del trattamento, poiché riceve il consenso dall'interessato assieme al mandato fiduciario per l'incarico o l'attività. Si pensi agli avvocati relativamente al contenzioso giudiziario, ovvero al medico che fornisca diagnosi e cura in regime libero professionale. È altresì vero, però, che molto spesso i professionisti erogano anche attività di consulenza ricevendo i dati da altro soggetto che ha a sua volta ricevuto il consenso al trattamento direttamente dall'interessato.

Basti pensare, ad esempio, al medico libero professionista che svolga attività di gestione del rischio sanitario ai sensi della legge Gelli - Bianco[23], ovvero sempre per rimanere in ambito sanitario, alle numerose consulenze giuridiche e ingegneristiche necessarie per il conseguimento dell' accreditamento di una struttura sanitaria presso il Servizio Sanitario Nazionale e il mantenimento dello stesso.

Tutti questi soggetti, anche data la loro alta specializzazione in materie specifiche, si trovano spesso ad esplicitare **attività di consulenza su particolari normative** (anche tecniche) trovandosi pertanto della situazione di agire in qualità di responsabile del trattamento per conto di più clienti quali autonomi e distinti titolari. Pertanto, come espressamente esplicitato dal garante, le informazioni di cui all'articolo 30, paragrafo 2 del **GDPR dovranno essere riportate nel registro con riferimento a ciascuno dei titolari, suddividendo il registro in tante sezioni quanti sono i titolari per conto dei quali**

[22] Per riferimenti il Garante ha predisposto una specifica ed esaustiva pagina di *frequenly asked questions* all'indirizzo: https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento#6 che contiene anche i modelli di registro semplificato per le PMI.

[23] Legge 24/2017 (cosiddetta Legge Gelli-Bianco dai nomi dei parlamentari che hanno completato l'iter) che regola la sicurezza delle cure e la responsabilità professionale. Tale normativa ha introdotto l'obbligatorietà del risk management per (ri)stabilire condizioni di assicurabilità delle strutture sanitarie. Il risk manager, nel settore della sanità privata, è di norma un professionista in regime di consulenza che assiste più strutture con mandati di regola ampi, avendo totale accesso a dati e archivi sanitari, procedure di cura, con possibilità di raccogliere dati direttamente dai pazienti per conto del titolare.

agisce. Nell'ambito della dimensione media degli studi professionali, é parere di chi scrive che non trovi applicazione il rinvio alle schede clienti, ma il garante esplicita comunque che "*ove, a causa dell'ingente numero di titolari per cui si operi, l'attività di puntuale indicazione e di continuo aggiornamento dei nominativi degli stessi nonché di correlazione delle categorie di trattamenti svolti per ognuno di essi risulti eccessivamente difficoltosa, il registro del responsabile potrebbe riportare il rinvio, ad es., a schede o banche dati anagrafiche dei clienti (titolari del trattamento), contenenti la descrizione dei servizi forniti agli stessi, ferma restando la necessità che comunque tali schede riportino tutte le indicazioni richieste dall'art. 30, par. 2 del RGPD*".

Questa ultima previsione del Garante, prevista ad esempio in caso di *software house* che svolgano attività di gestione informatica per un gran numero di clienti, sicuramente trova scarsa applicazione per gli studi professionali, anche quelli con maggior numero di clienti, dato che un singolo responsabile del trattamento libero professionista, trovandosi a dover erogare attività di consulenza ad un gran numero di clienti omogenei tra loro, probabilmente organizza il proprio lavoro in forma di impresa uscendo dalle forme proprie dello studio professionale.

2.6 L'art. 32: obbligo per il titolare del trattamento di adottare misure tecniche e organizzative adeguate per garantire un livello di sicurezza corrispondente al rischio.

Il Regolamento Europeo fa un primo riferimento alle misure di sicurezza già dell'articolo 22 dove, in linea con il principio di *accountability*, sposta in capo al titolare del trattamento la responsabilità di adottare (*rectius*: organizzare e costruire nel dettaglio) misure tecniche e organizzative *adeguate* ad una eventuale successiva dimostrazione di conformità alla norma.

Questo criterio aperto, di dichiarata **ispirazione alle normative volontarie** (come ad esempio quelle della famiglia delle ISO/IEC, impostate sul criterio del darsi una regola, metterla in pratica, verificarne l'efficacia e migliorare la regola stessa), costituisce **uno dei maggiori punti di rottura** rispetto all'impostazione delle normative a cui noi italiani siamo abituati. Infatti, per l'impostazione formalistica tradizionale della legislazione italiana, abituata a lunghi elenchi di adempimenti tassativi, un criterio aperto da adattare caso per caso, sul quale dibattere successivamente in sede di ispezione ed eventuale contestazione, nel quale la responsabilità non è ancorata all'esatto adempimento di una serie di obblighi ma alla corretta **interpretazione di principi aperti**, costituisce per l'operatore di *Civil Law* un vero e proprio salto nel buio.

Salto nel buio che viene agevolato solo in parte dal successivo disposto dell'articolo 32 che fornisce **alcuni rimedi che il titolare o il responsabile del trattamento dei dati potranno**

concretamente adottare, sempre tenuta in debito conto la valutazione di adeguatezza che resta in capo al titolare stesso.

Queste misure**, suggerite dall'art. 32, sono:**

1. **la pseudonimizzazione e cifratura dei dati personali**,
2. **la capacità di assicurare la continua riservatezza**, integrità disponibilità e resilienza dei sistemi e dei servizi che trattano i dati,
3. **la capacità di ripristinare tempestivamente** la disponibilità e l'accesso dei dati **in caso di incidente** fisico e tecnico, e
4. **una procedura per verificare e valutare le misure** tecniche e organizzative adeguate al fine di garantire la sicurezza dei trattamenti.

Se queste norme trovano facile riscontro nella cultura della consulenza aziendale, più che abituata all'adozione di sistemi di gestione e alla creazione di soluzioni su misura, declinare già solo le misure previste dall'articolo 32 del Regolamento comporta qualche problema applicativo in più. Ad esempio, quando parliamo di ***pseudonimizzazione del dato,*** ci riferiamo non tanto all'**attribuzione di un codice numerico ad ogni cliente** dello studio, pratica invero già di uso corrente in moltissime realtà professionali, ma a tutto quel complesso di misure che debbono portare in pratica ad evitare, ad esempio, che la segretaria dello studio medico chiami per cognome ad alta voce il paziente in sala d'attesa.

Quindi a fianco all'archivio ben ordinato con i codici a barre copertina sui fascicoli e la chiave saldamente riposta in tasca al personale, le misure tecniche e organizzative dovranno necessariamente prevedere una pur minima formazione del personale, un Regolamento interno di studio e così via.

Per quanto riguarda la **cifratura,** dato che stiamo parlando di studi professionali, è appena il caso di accennare che, qualora il professionista si avvalga di società esterne che offrono archivi in cloud cifrati, essendo il professionista stesso il titolare del trattamento dovrà accertarsi che chi offre l'archivio, opportunamente nominato responsabile, dia sufficienti garanzie in merito ad accesso e recupero dei dati su richiesta dal database cifrato.

Altri due concetti a cui fa riferimento articolo 32 del Regolamento, che a parere di chi scrive hanno bisogno di essere adattati per essere trasferiti dalla cultura aziendale a quella dello studio professionale a cui siamo abituati noi in Italia, sono quelli della **resilienza dei sistemi e dei servizi,** e la necessità di approntare un **sistema di *disaster recovery.***

Con riferimento a quanto detto precedentemente riguardo alla nozione di archivio, infatti, vediamo che per l'applicazione del principio dell'*accountability*, in capo al titolare e al responsabile, arriva anche

l'obbligo di assicurare la solidità dei propri sistemi e servizi. **Sistemi e servizi** che, **fin dalla progettazione, devono essere creati,** implementati o adattati **per garantire non solo problemi ai malintenzionati**, ma anche assicurare la **salvaguardia del dato contro fughe e perdite accidentali** dei dati stessi.

Anche qui, come visto sopra, l'obbligo della valutazione di adeguatezza in capo al professionista non consente di risolvere la situazione affidandosi, ad esempio, *in toto* ai servizi di qualche società esterna, ma comporta necessariamente la **gestione suppletiva e integrata dei servizi che si sono acquistati sul mercato, con le proprie procedure di studio e con il proprio personale di fiducia**, che deve essere debitamente formato e istruito.

Disaster recovery e *business continuity* sono due espressioni che possono essere declinate in italiano per la parte che ci interessa, come la capacità di reagire in modo efficace e tempestivo ad eventuali criticità dovute agli incidenti fisici tecnici, allo scopo di ripristinare la disponibilità e l'accesso dei dati personali oggetto di trattamento garantendo la continuità del servizio. Si tratta anche qui di unire la progettazione di processi logici con l'acquisto o la creazione di soluzioni informatiche, aggiungendo formazione e addestramento del personale.

In questo panorama, ideato e strutturato per realtà che in media sono ben più grandi dello *studio professionale con almeno un dipendente* che possiamo riscontrare nella casistica italiana, ancora una volta ci viene in aiuto il concetto di centralità dell'interessato. È l'interessato infatti, colui che il Regolamento mette al centro dell'incrocio tra obblighi e tutele. Tutte le misure che, sotto la propria responsabilità, titolari e responsabili dovranno costruire all'interno del proprio studio dovranno essere volte a garantire e agevolare l'esercizio dei propri diritti da parte dell'interessato.

Mentre sicuramente si può dire che il legislatore, sfilando il Regolamento con l'occhio alle grandi aziende magari che lavorano nel *big data*, abbia inteso titolare e responsabile quali destinatari di obblighi, visto il momento storico in cui una gestione troppo sportiva dei dati personali raccolti attraverso la rete ha portato a casi eclatanti, il professionista regolamentato è fin troppo abituato nel panorama italiano alla corretta gestione della propria responsabilità professionale quale soggetto responsabile verso il proprio cliente/interessato.

Non sfugge pertanto come proprio i professionisti regolamentati, nell' implementare le misure tecniche ma, anche e soprattutto organizzative dei propri studi siano culturalmente avvantaggiati rispetto al far west del panorama aziendale.

2.7 Sistemi di certificazione

Nel panorama dei sistemi di certificazione, **normative come la ISO 27001,** che definisce e gestisce un *sistema di gestione per la sicurezza delle informazioni*, **possono sicuramente essere d'aiuto** per la messa in sicurezza del proprio studio ai fini della conformità normativa con il Regolamento Europeo.

Conosciute tendenzialmente per il vantaggio competitivo che portano all'interno delle organizzazioni che ne mettono in pratica la corretta applicazione, le cosiddette normative volontarie sono ormai diventate di uso comune per la gran parte delle realtà aziendali, soprattutto data la loro **obbligatorietà di fatto**, ad esempio, **per la partecipazione a molte gare indette dalle varie stazioni appaltanti** pubbliche e private.

Tutte le normative della famiglia delle ISO propongono degli standard di comportamento, di servizio o di prodotto, contemporaneamente ad una serie di metodi di verifica tanto della situazione *quo ante* che *ex post* applicazione della normativa stessa. Si tratta, in buona sostanza, del concetto di *compliance:* si fissa una regola a far da parametro, si misura la distanza (c.d. *gap analysis*) tra la norma e la situazione di fatto, e si stabiliscono ed eseguono tutte le azioni correttive necessarie (acquisire un software, scrivere una procedura, approntare un corso di formazione, stabilire un calendario di ispezioni) per avvicinare quanto più possibile la realtà allo standard fissato nella regola.

In particolare il GDPR richiama in diversi punti principi e approcci propri delle ISO in generale e della 27000 in particolare. È di particolare interesse inoltre la circostanza che i sistemi di gestione costruiti in conformità alla norma, possono essere certificati da enti esterni appositamente accreditati che si fanno garanti del rispetto da parte del titolare o del responsabile certificato dei requisiti previsti dalle norme degli standard internazionali di guardo la conformità di prodotti, servizi, processi, sistemi e persone.

Gli articoli 42 e 43 del Regolamento dedicano ampio spazio alla certificazione e agli organismi di certificazione prevedendo perfino che gli stati membri e le autorità nazionali e comunitarie incoraggino l'istituzione dei mercati di certificazione, sigilli, marchi di protezione dei dati il cui ottenimento dovrà essere commisurato alle esigenze delle micro, piccole e medie imprese, o studi professionali nel nostro caso.

I punti di contatto saltano all'occhio con le certificazioni previste dall'articolo 43 del GDPR, che ricalcano lo schema triennale proprio delle normative ISO, con verifiche intermedie di conformità, rilascio e rinnovo.

In questo schema normativo, la difficoltà dell'interprete rimane quella di calare nella realtà del piccolo o piccolissimo studio professionale (che, ci corre l'obbligo di ricordare, rappresenta ancora la forma lavorativa scelta dalla stragrande maggioranza dei professionisti regolamentati) gli standard di

conformità pensati per organizzazioni complesse in cui l'adozione di un sistema di gestione velocizza e fluidifica il lavoro attraverso un riparto efficace di mansioni e competenze, invece di appesantire i flussi interni di una realtà con poche persone per cui il sistema di gestione si traduce inevitabilmente in una serie interminabile di adempimenti.

Vero è, d'altra parte, che le ISO in generale e la 27001 in particolare consentono di rispondere velocemente in modo efficace a molti dei quesiti aperti dalla formulazione del Regolamento Europeo fornendo preziosissimi strumenti pratici per costruire documenti interni, dare evidenza di processi e procedure, misurare i rischi e calibrare le contromisure.

In particolare, estremamente **prezioso tanto per chi voglia occuparsi in proprio della messa in sicurezza del proprio studio professionale, quanto del consulente** che si approcci alla messa in sicurezza degli studi professionali altrui, è **l'appendice all'ultima edizione della norma**, titolato ***obiettivi di controllo e controlli di riferimento***. Si tratta di una lunga elencazione di "obiettivi di controllo" ossia quei potenziali punti deboli dell'organizzazione che potrebbero presentare un *vulnus* per i diritti dell'interessato, Accanto agli stessi dei controlli, cioè delle modalità di verifica che il sistema ritiene congruo per la verifica della conformità normativa. Se il controllo da esito positivo ci troveremo di fronte ad una *conformità normativa*, ossia senza nessun obbligo ulteriore, se non una verifica periodica in seguito sullo stesso punto. Qualora invece il controllo fosse di esito negativo, dovremmo dare evidenza della non conformità alla data attuale, pianificare delle azioni decidendo la priorità dell'intervento, porre in essere le azioni tenendo traccia dell'attività svolta e pianificare una successiva verifica per testare il raggiungimento della conformità normativa.

Questa metodologia, conosciuta in inglese con l'espressione *plan-do-check-act* ci consente in teoria di gestire qualunque dimensione di studio o di azienda a seconda della complessità della stessa o della rischiosità della situazione di fatto. Si tratta In sostanza di un processo continuo di miglioramento dello stato dell'arte, di cui si trovano continui richiami nei principi generali del Regolamento Europeo assieme a molti altri punti di contatto.

Il sommesso consiglio di chi scrive, per concludere, è quello di utilizzare la norma come utile, utilissimo strumento di valutazione e autovalutazione in quanto applicabile alla propria realtà di studio, piuttosto che affannarsi alla costruzione di un ingombrante e costoso sistema di gestione, più adatto nella pratica a realtà di tipo aziendale che al modello di business dello studio professionale.

Cionondimeno, la ISO rimane uno strumento fondamentale per tutti quelli che, di fronte a criteri volutamente ampi come quelli proposte del Regolamento, abbiano bisogno di strumenti pratici per focalizzare la propria attività di messa a norma delle realtà in cui sono chiamati ad operare.

A una prima lettura gli adempimenti previsti dalla normativa, ed in particolare gli obiettivi di controllo, appaiono inevitabilmente sovradimensionati rispetto alla realtà dello studio professionale. A una lettura attenta, però troviamo come la metodologia proposta ed implementata all'interno delle normative volontarie (tutte non solo la ISO 27001), diventi una chiave di lettura dispensabile per tutti quelli che vogliono approcciarsi in modo scientifico e analitico a concetti come il *risk assessment* oppure l'*accountability* evitando il rischio da un lato di costruire fantasiose teorie di scarsa efficacia, oppure, dal lato opposto di soffocare se stessi o il titolare del trattamento per cui si lavora sotto una montagna di adempimenti spesso quasi identici l'uno all'altro.

3.

Protezione dei dati personali e tutela della privacy dei lavoratori

(Dott. Marco Miceli)

3.1 La privacy dei lavoratori

3.1.1 Analisi di contesto

Nell'ambito del rapporto di lavoro è fisiologico procedere alla raccolta e al trattamento di dati personali del lavoratore dipendente[24]. Tuttavia, il lavoratore – in quanto, soggetto interessato al trattamento[25] – ha il diritto di mantenere il costante "controllo" delle informazioni che lo riguardano e che sono raccolte dal datore di lavoro, fino al punto di poterne condizionare l'utilizzazione e di limitarne la diffusione.

TIPOLOGIE DI DATI TRATTATI DAL DATORE DI LAVORO	DESCRIZIONE DELLA TIPOLOGIA DI DATI TRATTATI	BASE GIURIDICA DEL TRATTAMENTO
Dati personali	qualsiasi informazione riguardante il lavoratore	L'art. 6 del GDPR enuncia le condizioni in base alle quali il trattamento può dirsi lecito[26].

[24] L'art.4 paragrafo 2 del GDPR contiene la definizione di trattamento: *"Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione"*.

[25] L'interessato al trattamento dei dati è, in poche parole, la persona fisica cui si riferiscono i dati personali oggetto di trattamento. L'interessato è, quindi, il destinatario finale della tutela predisposta dal Regolamento europeo per quanto riguarda le operazioni di trattamento dei dati personali.

[26] Art. 6 GDPR: *"1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:*
a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

Dati particolari	comprendono tutti quei dati personali idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, i dati genetici o biometrici tesi a identificare in modo univoco una persona fisica, i dati riguardanti la salute, la vita o l'orientamento sessuale della persona (ovvero i dati sensibili di cui al Codice Privacy prima dell'entrata in vigore del GDPR)	È richiesto il consenso esplicito dell'interessato. Tuttavia, ai sensi dell'art. 9 GDPR, il datore di lavoro può trattare questi dati se ricorrono "*motivi di rilevante interesse pubblico*", individuati dal D.Lgs. 101/2018. Si tratta dell'instaurazione, la gestione e l'estinzione di rapporti di lavoro di qualunque tipo (anche non retribuito) nonché dell'adempimento degli obblighi retributivi, fiscali e contabili, di igiene e sicurezza del lavoro.
Dati relativi a condanne penali e reati	Si pensi, ad esempio, al certificato penale per chi ha contatti diretti e regolari con minori, per verificare l'assenza di certi reati	Il trattamento dei dati personali relativi a condanne penali e reati è consentito solo se autorizzato da una norma di legge, da un Regolamento o, in mancanza, con apposito decreto del Ministro della Giustizia. Il datore di lavoro potrà trattare i dati relativi alle condanne penali solo per l'adempimento di obblighi di legge in materia di diritto del lavoro.

Il controllo **che il lavoratore dipendente/soggetto interessato esercita sul trattamento dei dati** che lo riguardano, rappresenta un vero e proprio **limite per il datore di lavoro/titolare del trattamento**, un limite che si sostanzia in quel diritto dei lavoratori alla riservatezza, nonché alla tutela della dignità personale, alla libertà di espressione e di comunicazione, e che trova applicazione rispetto al potere di controllo che legittimamente esercita il datore di lavoro, sia in ordine alla prestazione del dipendente per l'esercizio del potere disciplinare, oltre che di quello organizzativo e direttivo (nel segno degli artt. 2086 e 2094 del Codice civile) sia per la tutela dei beni aziendali.

---

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.
La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti".

Un **contemperamento di diritti contrapposti** che - a ben vedere – trova già riconoscimento nella Legge n. 300 del 1970 (Statuto dei Lavoratori) che – come noto – disciplina e regolamenta i poteri del datore di lavoro[27].

Non v'è dubbio che per effetto dell'evoluzione tecnologica, soprattutto attraverso *smartphone* e *tablet*, risulti assai favorita l'interazione in mobilità senza che sia più necessario l'utilizzo del "classico" computer. Ciò ha comportato un **ampliamento delle modalità di raccolta e di comunicazione di dati**, sempre più spesso basate su immagini e contenuti multimediali, con un conseguente impatto sul comportamento delle persone nella loro quotidianità. Parimenti indubbio è che siamo difronte a una svolta evolutiva con ricadute di notevole vantaggio sociale, percepibili sia nel contesto personale che in quello lavorativo.

Basti pensare all'utilizzo degli strumenti – ormai necessari – cui facciamo continuo ricorso, anche nelle ore notturne. Ciononostante, in troppi casi, si registra il rischio di una involuzione: l'utilizzo di *app* spesso poco sicure e foriere di rischi connessi alla sicurezza dei dati (a ciò si aggiunge la gratuità – apparente! - di tali servizi che ne aumenta, a livello esponenziale, l'*appeal*).

[27] Gli articoli 4 e 8 dello Statuto dei lavoratori assicurano la tutelare contro i controlli del lavoratore e garantiscono la sfera di riservatezza nel rispetto degli articoli 1, 2, 6, 13, 14 e 15 della Costituzione.

In particolare, l'art. 8 dello Statuto dei Lavoratori vieta al datore di lavoro l'indagine sulle opinioni (politiche, sindacali, religiose etc.) del lavoratore.

Invece, l'art. 4 (modificato dall'art. 23 D.Lgs. 151/2015 e, successivamente, dal D.Lgs. 185 del 2016, c.d. decreto correttivo, in modifica del D.Lgs. n. 151 del 2015) limita il potere di controllo a distanza, ovvero da remoto, dell'attività dei lavoratori. Un tema particolarmente dibattuto è proprio quello che attiene ai sistemi di videosorveglianza del lavoratore, tanto che già nella Relazione ministeriale al disegno di legge dello Statuto dei lavoratori viene affermato che la sorveglianza debba essere *"mantenuta in una dimensione umana e cioè non esasperata dall'uso delle tecnologie che possono rendere la vigilanza stessa continua e anelastica, eliminando ogni zona di riservatezza e di autonomia nello svolgimento del lavoro"*. L'Autorità Garante per la Protezione dei Dati Personali aveva affrontato la questione con il provvedimento generale del 2010 che continua a trovare applicazione anche se precedente al D.lgs. 101/2018 che ha adeguato il Codice Privacy al GDPR. Il Provvedimento in materia di videosorvegianza del Garante per la privacy è consultabile al seguente link:

https://www.garanteprivacy.it/documents/10160/10704/Provvedimento+in+materia+di+videosorveglianza+-+leaflet+.pdf/6c3df7ec-7f25-4d5f-9ef9-eaebf6e9f0df?version=1.2

Per completezza, anticipiamo – quanto sarà oggetto di approfondimento nel paragrafo 3.3, ovvero - che in materia di videosorveglianza in ambiente lavorativo, il Comitato Europeo per la Protezione dei Dati (EDPB) ha adottato il 10 giugno 2019 le linee-guida sulla videosorveglianza che chiariscono in quali termini il GDPR si applichi al trattamento dei dati personali quando si utilizzano dispositivi video, e mirano a garantire l'applicazione coerente del GDPR in materia. Le linee-guida riguardano sia i dispositivi video tradizionali sia i dispositivi video intelligenti. Per quanto concerne questi ultimi, le linee-guida si concentrano sulle norme relative al trattamento di categorie particolari di dati. Si tratta di un documento oggetto di una consultazione pubblica, rispetto alla quale potranno essere inviati commenti all'indirizzo EDPB@edpb.europa.eu entro e non oltre il 09/09/2019.

Per effetto del Regolamento UE 2016/679 e del D.Lgs. 101/2018 che ha adeguato la normativa nazionale alle disposizioni del menzionato Regolamento generale[28] è stato posto in essere un sistema normativo che vieta i controlli lesivi dei diritti inviolabili e qualunque tipo di controllo occulto o a distanza nei confronti dei lavoratori[29].

La trasformazione del mondo del lavoro, cui stiamo assistendo negli ultimi anni, continua a riflettersi sulle dinamiche che tipicamente caratterizzano il rapporto di lavoro, presentando sul tavolo di coloro che - come me - si occupa di organizzazione e *Human Resource Management* una serie di sfide dal carattere avvincente, tra queste spiccano i modelli di ***Smart working*** **e** *Bring Your Own Device* (BYOD).[30]

Si tratta, certamente, di due istituti in virtù dei quali numerosi contesti lavorativi e aziendali sono riusciti a varcare le nuove frontiere della *digital economy* per approdare a quella che molti definiscono la quarta rivoluzione industriale.

Il dibattito in corso sulla valutazione "costi – benefici" che l'adozione di tali modelli comporta per l'azienda e per i lavoratori, non può non prendere in considerazione gli aspetti critici e gli adempimenti che si rendono necessari sotto il profilo della sicurezza informatica aziendale e il rispetto della protezione dei dati personali dei lavoratori.

In relazione al profilo della sicurezza informatica aziendale, si rileva che **una parte considerevole degli attacchi informatici** che le aziende (e gli studi professionali) subiscono è a causa di quell'uso promiscuo – per fini personali e professionali – del *device* in dotazione al lavoratore.

[28] A partire dal 25 maggio 2018, per effetto dell'entrata in vigore del Regolamento è scaturita la disapplicazione delle disposizioni del Codice Privacy incompatibili con lo stesso, si tratta dei cd casi di antinomia tra leggi *self-executing* europee e leggi ordinarie italiane.

[29] Si segnala, sul fronte opposto: MASSIMA TRIBUNALE SEZ. LAV. - PADOVA, 22/01/2018 *"Ipotesi di controlli leciti non soggetti alle condizioni di cui all'art. 4 st. lav. In materia di controlli difensivi ad opera del datore di lavoro, residua un'area di controlli difensivi leciti non soggetti alle condizioni di cui all'art. 4, c. 1, l. 300/1970. Tale ambito è determinato dall'acquisizione di indizi del compimento di condotte illecite a carico di singoli dipendenti, in danno del datore di lavoro o per le quali possa essere chiamata a rispondere il datore di lavoro"*. Fonte: Redazione Giuffrè 2019

[30] *Smart working* è la definizione inglese di *"lavoro agile"* previsto e disciplinato dalla Legge n. 81/2017, un istituto giuridico che attribuisce all'attività lavorativa caratteri di flessibilità e dinamismo, al punto da ridurre i vincoli di tempo e attenuare la tradizionale distinzione tra luogo di lavoro e ambiente domestico . *Bring your own device* (BYOD) è, invece, la definizione inglese del modello che consente ai lavoratori di portare i propri dispositivi personali nel posto di lavoro e viceversa, affinchè possano avere accesso continuo alle informazioni relative alla propria attività lavorativa. In effetti, la traduzione letterale in italiano è: "porta il tuo dispositivo".

In relazione al profilo che attiene al rispetto della protezione dei dati personali dei lavoratori, non può escludersi che si possa configurare un'azione di ***controllo a distanza dell'attività del lavoratore*, non sempre conforme a quanto sancito dalla normativa** giuslavoristica[31].

Proprio rispetto a questo ultimo profilo di rischio - la protezione dei dati personali dei lavoratori – si deve evidenziare che, stante la modifica dell'art. 4 dello Statuto dei Lavoratori e fino all'entrata in vigore del GDPR, non si erano posti problemi di "sovrapposizione" tra la disciplina giuslavoristica dei controlli a distanza e la tutela dei dati personali, le quali sembravano viaggiare su due binari perfettamente paralleli.

A partire dal 25 maggio 2018, invece, emergono delle vere e proprie **aree di intersezione**: l'utilizzabilità dei dati personali raccolti dal datore di lavoro è subordinata al rispetto di quei nuovi adempimenti disposti dal Regolamento UE 2016/679 e dall'impianto normativo che è scaturito per effetto dell'abrogazione di quelle norme del Codice Privacy incompatibili con lo stesso GDPR[32].

Sul piano generale, **il datore di lavoro** che eserciti il trattamento dei dati personali dei propri dipendenti **dovrà assicurare il rispetto dei diritti fondamentali dei lavoratori e, per far ciò, dovrà individuare correttamente la base giuridica del trattamento** stesso, ovvero:

1. adempimento di obblighi derivanti da un contratto di lavoro;
2. adempimento di obblighi previste dalla legge;
3. interesse legittimo del datore di lavoro – in quanto titolare del trattamento - o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato e la loro protezione.

Nel primo caso, l'onere della prova grava sul titolare del trattamento, il quale è obbligato a predisporre una dichiarazione scritta chiara e facilmente comprensibile per l'interessato, che dovrà

[31] Cfr.: art. 4 Legge n. 300/1970, modificato dal D.Lgs. n. 151/2015 e art. 21 della già menzionata Legge n. 81/2017, nonché nota del Ministero del Lavoro del 18 giugno 2015.

Un esempio eclatante di controllo a distanza dei lavoratori è quello noto come il "caso braccialetto elettronico" che, dopo aver riguardato Amazon, si è riproposto – seppur in misura molto ridotta – anche in Italia: una società che si occupa della raccolta dei rifiuti per conto della municipalizzata di un comune toscano aveva dotato i propri operatori ecologici di un braccialetto elettronico in grado di connettersi con i 2.500 nuovi cestini della spazzatura installate sul territorio per "certificarne" lo svuotamento. Senonché, il Garante, dopo aver espresso il suo parere contrario sull'uso dei braccialetti elettronici, ha chiesto l'adozione di dispositivi alternativi che non danneggino la dignità dei lavoratori.

[32] Nel Capo II del Regolamento UE 2016/679 vengono indicati i principi da rispettare, al fine di acquisire lo *status* di *"gdpr compliant"*.

essere sottoscritta in piena libertà. Una circostanza, quest'ultima, che chiaramente non si configura nel caso del lavoratore dipendente, in quanto soggetto debole[33].

Il secondo caso, invece, si attaglia perfettamente al rapporto di lavoro, in considerazione del fatto che l'esecuzione del **contratto di lavoro rende necessario il trattamento dei dati** dell'interessato/dipendente, inoltre, il versamento delle ritenute fiscali a carico del datore di lavoro - in qualità di sostituto d'imposta - fa ricadere nella stessa categoria, di obbligo legale, il trattamento dei dati personali.

Infine, in relazione al trattamento di dati personali basato sul **legittimo interesse del datore di lavoro, è richiesta la preventiva valutazione** di quest'ultimo, volta a verificare che il trattamento stesso sia necessario e proporzionato per il perseguimento di una legittima finalità, quindi la prescritta redazione del piano di valutazione di impatto rischio privacy, così come previsto dall'art. 35 GDPR.[34] Resta comunque salvo il diritto dei dipendenti di opporsi al trattamento.

3.1.2 DPIA per il datore di lavoro/titolare del trattamento

L'obbligo della "*Valutazione d'impatto sulla protezione dei dati"* (*Data Protection Impact Assessment* – DPIA)[35] secondo le Linee Guida del documento *Working Party 29* n.24824, si configura **in alcuni casi specificamente indicati,** tra cui il caso di **trattamento di dati sensibili** e il **monitoraggio continuo** dei dipendenti, anche **attraverso sistemi di videosorveglianza.**

---

[33] L'obiezione che viene mossa nei confronti di quanti sostengono che il datore di lavoro, oltre a consegnare al proprio dipendente l'informativa, dovrebbe comunque raccogliere il consenso al trattamento dei dati si fonda sul fatto che tale consenso non sarebbe opponibile in caso di contenzioso perché il lavoratore è - di fatto – in una situazione di "soggezione" per cui sottoposto a una pressione tale che impedirebbe a quel consenso di connotarsi come prestato in piena libertà.

[34] L'obbligo di valutazione che grava sul datore di lavoro – e, più in generale, su ogni titolare del trattamento – realizza il principio generale di "responsabilizzazione" che il Legislatore comunitario definisce con l'espressione *accountability*. In pratica, il titolare del trattamento deve valutare in piena autonomia la conformità e l'adeguatezza del trattamento e deve sempre essere in grado di dimostrare di non essere inadempiente. L'obbligo di elaborazione preventiva della DPIA si configura in tre casi specifici ovvero: il trattamento automatizzato dei dati, compresa la profilazione, che produce effetti giuridici sugli interessati; il trattamento su larga scala di categorie particolari di dati e la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

[35] Lo specifico argomento che attiene "Valutazione d'impatto sulla protezione dei dati" sarà oggetto di una approfondita analisi nell'ambito del Capitolo 4; in questa sede se ne tratta esclusivamente in relazione al tema focale che vuole essere quello della raccolta di immagini e videosorveglianza in ambiente lavorativo.

"VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI" **(*Data Protection Impact Assessment* – DPIA)**	
Contenuto minimo e descrizione dell'obbligo	La DPIA descrive, in maniera sistematica, i trattamenti previsti specificandone le finalità che può anche essere quella dell'interesse legittimo. Inoltre, la DPIA contiene la valutazione della necessità e proporzionalità dei trattamenti in base alle finalità, i rischi anche solo potenziali in ordine alla tipologia di dati trattati; le misure di sicurezza poste in essere dal titolare del trattamento nonchè gli eventuali rischi residui non eliminabili. Attenzione: ai sensi del paragrafo 11 dell'art. 35 GDPR, vige l'obbligo di rielaborazione del documento almeno nei casi in cui dovessero registrarsi variazioni. In pratica, per poter "comprovare" di essere *compliant*, il titolare del trattamento dovrà porre in porre in essere un'attività di monitoraggio e di revisione continui. Ecco perché si suole definire "dinamici" gli obblighi in materia di privacy, contrapponendo tale aggettivo a quello di "statico" che si attaglia, invece, a quelli la cui natura è caratterizzata dal fatto di potervi adempiere a scadenze programmate e calendarizzate (ad esempio, gli obblighi fiscali).
Si segnala che tramite il sito istituzionale del Garante per la Protezione dei Dati Personali è possibile accedere – in modalità *open source* - al *software* per l'elaborazione della valutazione d'impatto. Si tratta di un software elaborato dal CNIL francese, disponibile anche il lingua italiana.	

Il Garante della Privacy, il 23 novembre 2006, aveva già adottato un **primo provvedimento generale** relativo al trattamento dei dati personali nell'ambito del rapporto di lavoro privato. Per effetto delle Linee guida del 2006[36] si punta – come si legge nella *premessa* - a *"fornire indicazioni e raccomandazioni con riguardo alle operazioni di trattamento effettuate con dati personali (anche sensibili) di lavoratori operanti alle dipendenze di datori di lavoro privati il Garante ravvisa l´esigenza di adottare le presenti linee guida, suscettibili di periodico aggiornamento, nelle quali si tiene conto, altresì, di precedenti decisioni dell´Autorità"*.

Il provvedimento in argomento riguarda i seguenti ambiti di operatività:

a) **la condotta del datore** di lavoro che deve trattare i dati personali dei propri dipendenti **nel rispetto dei principi di liceità, trasparenza, pertinenza e finalità;**

[36] Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati. (Deliberazione n. 53 del 23 novembre 2006). Consultabili al seguente link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1364939

b) **le modalità di comunicazione** dei dati, funzionale all'esecuzione degli obblighi derivanti dal contratto di lavoro o degli obblighi di legge e l'informativa che il datore di lavoro deve rendere[37];

c) **l'individuazione dei soggetti che possono legittimamente intervenire** nel trattamento dei dati. Si pensi, oltre al titolare e responsabile del trattamento, al medico competente per quanto attiene ai dati di tipo sanitario e ai sistemi di delega da adottarsi nei contesti di gruppo d'impresa a favore di ciascuna delle società del gruppo – che agisce a titolo di responsabile del trattamento - per lo svolgimento di adempimenti in materia di lavoro, previdenza ed assistenza sociale;

d) le **tipologie di dati personali** dei lavoratori, distinguendo tra quelli che possono essere trattati dal datore di lavoro che può avere accesso in pendenza del rapporto di lavoro per le finalità di esecuzione del contratto e quei dati il cui trattamento è vietato al datore di lavoro, come nel caso dei dati sanitari idonei a rivelare lo stato di salute del lavoratore, oppure quelli relativi al credo religioso o all´adesione a sindacati.

Questi dati sono contenuti in atti o documenti che il lavoratore ha fornito al momento dell'assunzione, resi disponibili in albi, bacheche o assunti dal datore di lavoro.

Sul piano operativo, dunque è indispensabile che il datore di lavoro/titolare del trattamento assicuri il giusto bilanciamento tra interessi di sicurezza aziendale e garanzie di protezione dei dati personali dei lavoratori dell'azienda stessa[38]. Un bilanciamento che dovrà scaturire come risultato di quel processo di *Data Protection Impact Assessment,* il cui contenuto, quindi, dovrà:

- rispettare i principi di *privacy by design* e *privacy by default* (art. 25 GDPR) dando dimostrazione – comprovando – di aver adottato misure tecniche e organizzative di sicurezza per la tutela dei dati del dipendente, a partire già dalla progettazione del sistema di monitoraggio dei dispositivi aziendali e nel rispetto del principio di minimizzazione dei dati (sul piano pratico, si consiglia di provvedere alla mappatura di tutti i dispositivi in uso ai dipendenti);

[37] Si segnala che in tale contesto, il Garante ha giudicato sproporzionata l'indicazione sul cartellino di dati identificativi nei rapporti con il pubblico.

[38] Si segnala: Massima Cassazione Civile Sez. Lav. - 21/08/2018, N. 20879 *"Il controllo a distanza del lavoratore tramite le timbrature del badge aziendale Il controllo del dipendente per il tramite della rilevazione dei dati di entrata e di uscita attraverso le timbrature del badge aziendale, ove tale modalità non sia concordata preventivamente con le rappresentanze sindacali ed ove si traduca in un controllo sul 'quantum' della prestazione lavorativa, è illegittimo e viola i limiti di cui all'art. 4 St. lav. ante riforma. Diversamente, è legittimo l'impiego delle risultanze del badge ove finalizzato allo svolgimento di indagini aventi ad oggetto fatti illeciti del dipendente, fra cui l'utilizzo abusivo del badge aziendale".* Fonte: Rivista Italiana di Diritto del Lavoro 2018, 4, II, 811.

- **rispettare il principio di *accountability***, al punto che il titolare del trattamento/ datore di lavoro, su richiesta dell'autorità di controllo, sarà in grado di "comprovare" cioè di dare prova che le scelte operate per assicurare la sicurezza dell'azienda siano coerenti con gli adempimenti previsti a suo carico per la protezione dei dati personali dei lavoratori dipendenti (sul piano pratico, si consiglia l'adozione di un'apposita informativa per i dipendenti);
- **prevedere l'adozione di misure tecniche e organizzative adeguate** *ex* art. 32 GDPR (per esempio, si consiglia di redigere una *policy* sulle modalità di utilizzo, da parte del dipendente, del *device* che riceve in dotazione, in particolare, si può prevedere l'obbligo di impostare una password per lo sblocco dello *smartphone* o la cifratura dei dati aziendali).
- **indicare la procedura interna da attuare in caso di *data breach* (**artt. 33 e 34 GDPR) sul *device* che il lavoratore riceve in dotazione (per esempio, si consiglia di redigere un protocollo di azione da seguire nei casi furto o smarrimento di un dispositivo portatile, telefono, *tablet*, memoria USB);
- **programmare e attuare la prescritta attività di formazione del personale** dipendente in materia di protezione dei dati personali, con particolare attenzione alla prevenzione del rischio privacy e alle azioni utili a mitigarne i danni, come previsto dagli artt. 29 e 32 GDPR (per esempio, si consiglia un approfondimento sulla pericolosità degli attacchi informatici di c.d. *phishing* che si innescano a causa di email fraudolente che contengono *link* malevoli o che rimandano a pagine web clonate, con l'obiettivo di indurre l'utente inconsapevole a digitare le proprie credenziali aziendali o che lo convincono a scaricare sul dispositivo aziendale allegati infetti).

3.2 Il Provvedimento generale del Garante in merito al trattamento di categorie particolari di dati, nei rapporti di lavoro

Al termine del prescritto periodo di consultazione (avviato pubblicamente dal Garante per la protezione dei dati personali il 13 dicembre 2018 e conclusosi lo scorso 5 giugno 2019) in Gazzetta Ufficiale Serie Generale del 29 luglio 2019, n. 176, è stato pubblicato, il "*Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101*"[39].

[39] Il Provvedimento generale del Garante in merito al trattamento di categorie particolari di dati tratta dei seguenti argomenti: prescrizioni relative al trattamento nei rapporti di lavoro (con riferimento all'autorizzazione generale 1/2016); prescrizioni relative al trattamento da parte degli organismi di tipo associativo, fondazioni, chiese e comunità religiose (con riferimento all'autorizzazione generale 3/2016); prescrizioni relative al trattamento da parte degli investigatori privati (con riferimento all'autorizzazione generale 6/2016); prescrizioni relative al trattamento

Obiettivo del documento e della propedeutica consultazione è quello di stabilire il destino delle prescrizioni – pre Regolamento (UE) 2016/679 (GDPR) – in materia di trattamento dei dati personali *ex sensibili,* ora – come definiti dal GDPR - *particolari*[40]. Di conseguenza, *cessano di produrre effetti dal momento della pubblicazione del Provvedimento*: le Autorizzazioni generali nn. 2/2016, 4/2016, 5/2016 (riguardanti rispettivamente: il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale, il trattamento dei dati sensibili da parte dei liberi professionisti e il trattamento dei dati sensibili da parte di diverse categorie di titolari) e la 7/2016 (relativa ai dati giudiziari) poiché *ritenute incompatibili con le disposizioni del Regolamento (UE) 2016/679.*

Per quanto attiene alla materia oggetto di questa mia analisi, si deve rilevare che il provvedimento *de quo* contiene le prescrizioni che riguardano il trattamento delle categorie particolari di dati nei rapporti di lavoro, specificandone l'ambito soggettivo in cui lo stesso si deve applicare, nonché le categorie dei soggetti interessati agli effetti della sua applicazione, oltre alle finalità e alle relative modalità di trattamento dei dati particolari, effettuato nell'ambito del rapporto di lavoro.

PRESCRIZIONI RELATIVE AL TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI NEI RAPPORTI DI LAVORO (AUT. GEN. N. 1/2016)	
AMBITO DI APPLICAZIONE Il presente provvedimento si applica nei confronti di tutti coloro che, a vario titolo (titolare/responsabile del trattamento), effettuano trattamenti per finalità d'instaurazione, gestione ed estinzione del rapporto di lavoro,	a) agenzie per il lavoro e altri soggetti che, in conformità alla legge, svolgono, nell'interesse di terzi, attività di intermediazione, ricerca e selezione del personale o supporto alla ricollocazione professionale ivi compresi gli enti di formazione accreditati; b) persone fisiche e giuridiche, imprese, anche sociali, enti, associazioni e organismi che sono parte di un rapporto di lavoro o che utilizzano prestazioni lavorative anche atipiche, parziali o temporanee, o che comunque conferiscono un incarico professionale alle figure indicate al successivo punto 1.2, lettere c) e d); c) organismi paritetici o che gestiscono osservatori in materia di lavoro, previsti dalla normativa dell'Unione europea, dalle leggi, dai regolamenti o dai contratti collettivi anche aziendali; d) rappresentante dei lavoratori per la sicurezza, anche territoriale e di sito; e) soggetti che curano gli adempimenti in materia di lavoro, di previdenza ed assistenza sociale e fiscale nell'interesse di altri soggetti che sono parte di un rapporto di lavoro dipendente o

dei dati genetici (con riferimento all'autorizzazione generale 8/2016) e prescrizioni relative al trattamento per scopi di ricerca scientifica (con riferimento all'autorizzazione generale 9/2016). Il testo del rovvedimento è consultabile al seguente link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9124510

[40] Tali prescrizioni sono il contenuto delle 9 Autorizzazioni generali, adottate il 15 dicembre 2016, che individuavano le garanzie e le misure appropriate e specifiche da adottare nel trattamento di dati che il GDPR definisce appartenenti alle *categorie particolari di dati personali* e di *dati personali relativi a condanne penali e reati* (artt. 9 e 10, GDPR).

in particolare:	autonomo, ai sensi della legge 11 gennaio 1979, n. 12, che disciplina la professione di consulente del lavoro; f) associazioni, organizzazioni, federazioni o confederazioni rappresentative di categorie di datori di lavoro, al solo fine di perseguire scopi determinati e legittimi individuati dagli statuti di associazioni, organizzazioni, federazioni o confederazioni rappresentative di categorie di datori di lavoro o dai contratti collettivi in materia di assistenza sindacale ai datori di lavoro; g) medico competente in materia di salute e sicurezza sul lavoro, che opera in qualità di libero professionista o di dipendente del datore di lavoro o di strutture convenzionate.
INTERESSATI AI QUALI I DATI SI RIFERISCONO Il presente provvedimento si applica ai trattamenti di categorie particolari di dati personali, acquisiti di regola direttamente presso l'interessato, riferiti a:	a) candidati all'instaurazione dei rapporti di lavoro, anche in caso di curricula spontaneamente trasmessi dagli interessati ai fini dell'instaurazione di un rapporto di lavoro (art. 111-bis del Codice); b) lavoratori subordinati, anche se parti di un contratto di apprendistato, di formazione, a termine, di lavoro intermittente, di lavoro occasionale ovvero praticanti per l'abilitazione professionale, ovvero prestatori di lavoro nell'ambito di un contratto di somministrazione di lavoro, o in rapporto di tirocinio, ovvero ad associati anche in compartecipazione; c) consulenti e liberi professionisti, agenti, rappresentanti e mandatari; d) soggetti che svolgono collaborazioni organizzate dal committente, o altri lavoratori autonomi in rapporto di collaborazione, anche sotto forma di prestazioni di lavoro accessorio, con i soggetti indicati nel precedente punto 1.1.; e) persone fisiche che ricoprono cariche sociali o altri incarichi nelle persone giuridiche, negli enti, nelle associazioni e negli organismi indicati nel precedente punto 1.1.; f) terzi danneggiati nell'esercizio dell'attività lavorativa o professionale; g) terzi (familiari o conviventi dei soggetti di cui alla precedente lett. b) e d) per il rilascio di agevolazioni e permessi.
FINALITÀ DEL TRATTAMENTO Il trattamento delle categorie particolari di dati personali è effettuato solo se necessario (art.9, par. 2 Regolamento UE	a) per adempiere o per esigere l'adempimento di specifici obblighi o per eseguire specifici compiti previsti dalla normativa dell'Unione europea, da leggi, da regolamenti o da contratti collettivi anche aziendali, ai sensi del diritto interno, in particolare ai fini dell'instaurazione, gestione ed estinzione del rapporto di lavoro (art. 88 del Regolamento UE 2016/679), nonché del riconoscimento di agevolazioni ovvero dell'erogazione di contributi, dell'applicazione della normativa in materia di previdenza ed assistenza anche integrativa, o in materia di igiene e sicurezza del lavoro, nonché in materia fiscale e sindacale; b) anche fuori dei casi di cui alla lettera a), in conformità alla legge e per scopi determinati e legittimi, ai fini della tenuta della contabilità o della corresponsione di stipendi, assegni, premi, altri emolumenti, liberalità o benefici accessori;

2016/679):	c) per perseguire finalità di salvaguardia della vita o dell'incolumità fisica del lavoratore o di un terzo; d) per far valere o difendere un diritto, anche da parte di un terzo, in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione, nei casi previsti dalle leggi, dalla normativa dell'Unione europea, dai regolamenti o dai contratti collettivi, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento; il trattamento di dati personali effettuato per finalità di tutela dei propri diritti in giudizio deve riferirsi a contenziosi in atto o a situazioni precontenziose; resta salvo quanto stabilito dall'art. 60 del Codice; e) per adempiere ad obblighi derivanti da contratti di assicurazione finalizzati alla copertura dei rischi connessi alla responsabilità del datore di lavoro in materia di salute e sicurezza del lavoro e di malattie professionali o per i danni cagionati a terzi nell'esercizio dell'attività lavorativa o professionale; f) per garantire le pari opportunità nel lavoro; g) per perseguire scopi determinati e legittimi individuati dagli statuti di associazioni, organizzazioni, federazioni o confederazioni rappresentative di categorie di datori di lavoro o dai contratti collettivi, in materia di assistenza sindacale ai datori di lavoro.
PRESCRIZIONI SPECIFICHE RELATIVE ALLE DIVERSE CATEGORIE DI DATI	▪ Trattamenti effettuati nella fase preliminare alle assunzioni; ▪ Trattamenti effettuati nel corso del rapporto di lavoro.
PRESCRIZIONI SPECIFICHE RELATIVE ALLE MODALITÀ DI TRATTAMENTO Con riferimento alle modalità di trattamento, si rappresenta quanto segue:	a) i dati devono essere raccolti, di regola, presso l'interessato; b) in tutte le comunicazioni all'interessato che contengono categorie particolari di dati devono essere utilizzate forme di comunicazione anche elettroniche individualizzate nei confronti di quest'ultimo o di un suo delegato, anche per il tramite di personale autorizzato. Nel caso in cui si proceda alla trasmissione del documento cartaceo, questo dovrà essere trasmesso, di regola, in plico chiuso, salva la necessità di acquisire, anche mediante la sottoscrizione per ricevuta, la prova della ricezione dell'atto; c) i documenti che contengono categorie particolari di dati, ove debbano essere trasmessi ad altri uffici o funzioni della medesima struttura organizzativa in ragione delle rispettive competenze, devono contenere esclusivamente le informazioni necessarie allo svolgimento della funzione senza allegare, ove non strettamente indispensabile, documentazione integrale o riportare stralci all'interno del testo. A tal fine dovranno essere selezionate e impiegate modalità di trasmissione della documentazione che ne garantiscano la ricezione e il relativo trattamento da parte dei soli uffici o strutture organizzative competenti e del solo personale autorizzato; d) quando per ragioni di organizzazione del lavoro, e nell'ambito della predisposizione di turni di servizio, si proceda a mettere a disposizione a soggetti diversi dall'interessato (ad esempio, altri colleghi) dati relativi a presenze ed assenze dal servizio, il datore di

	lavoro non deve esplicitare, nemmeno attraverso acronimi o sigle, le causali dell'assenza dalle quali sia possibile evincere la conoscibilità di particolari categorie di dati personali (es. permessi sindacali o dati sanitari).

3.3 Videosorveglianza in ambiente lavorativo

Una delle più interessanti – quanto dibattute - "aree di intersezione" tra la normativa giuslavoristica e quella che attiene alla tutela della privacy è rappresentata dalla videosorveglianza in ambiente lavorativo.

Aziende e studi professionali, sempre più spesso, avvertono la **necessità di installare telecamere di sorveglianza** che inquadrino determinate aree della struttura.

Se è vero – come è vero – che **il fine è quello di mettere in sicurezza e prevenire furti, violazioni** e intrusioni, è altrettanto vero che – in alcuni casi - il datore di lavoro tenda a sfruttare le telecamere sul posto di lavoro per controllare i propri dipendenti e per valutarne la produttività lavorativa, si tratta del cosiddetto ***"secondary use"*.**

L'installazione di sistemi di videosorveglianza in ambiente lavorativo comporta la piena conoscenza e il rispetto della normativa vigente: lo **Statuto dei lavoratori, in particolare, l'art. 4** che **pone un divieto generale del controllo a distanza** dell'attività dei lavoratori e la normativa sulla privacy, quindi del Regolamento UE 2016/679, il Codice della Privacy (D.Lgs n.196/2003 così come modificato per effetto del D.Lgs. 101/2018) nonché le Circolari del Ministero del Lavoro[41], i Provvedimenti del Garante per la privacy[42] e quelli dell'*European Data Protection Board* (EDPB), ultimo – in ordine di tempo - le linee guida 3/2019 del 12 luglio 2019 sul trattamento dei dati personali in merito ai servizi di videosorveglianza[43].

Sulla base del vigente quadro normativo, dunque, il datore di lavoro potrà svolgere una attività di controllo sui lavoratori solo se dimostrerà di **rispettare i seguenti principi in materia di tutela dei dati personali.**

[41] Si segnalano: la nota n. 299 del 28 novembre 2017 e la circolare n. 5 del 19.02.2018, entrambi, dell'Ispettorato Nazionale del Lavoro. Quest'ultima consultabile al seguente link: https://www.ispettorato.gov.it/it-it/orientamentiispettivi/Documents/Circolari/INL-Circolare-n-5-del-19-febbraio-2018-Videosorveglianza-signed.pdf

[42] Per la consultazione di documenti del Garante privacy in materia di videosorveglianza si consiglia il seguente link: https://www.garanteprivacy.it/home/ricerca/-/search/key/videosorveglianza

[43] Il testo in lingua inglese delle linee guida può essere consultato sul sito:

https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf

PRINCIPIO	CONDOTTA DEL DATORE DI LAVORO CONFORME
Principio di necessità	Il controllo deve risultare necessario o indispensabile rispetto a uno scopo determinato e avere il carattere dell'eccezionalità, limitato nel tempo e nell'oggetto, mirato e mai massivo.
Principio di finalità	Il controllo deve essere finalizzato a garantire la sicurezza o la continuità aziendale, o a prevenire e reprimere condotte illeciti dei lavoratori.
Principio di trasparenza	Il datore di lavoro è obbligato a dare informazione preventiva ai dipendenti circa le modalità e i limiti di utilizzo degli strumenti di lavoro nonché delle sanzioni previste nel caso di violazione di tali limiti.
Principio di proporzionalità	Il datore di lavoro è obbligato ad adottare forme di controllo che risultino essere strettamente proporzionate - e non eccedenti – rispetto alla finalità che giustifica tale attività di controllo.
Principio di sicurezza	Tutti i dati raccolti devono essere protetti in modo adeguato.

Soffermando la nostra attenzione all'analisi del dato normativo, deve evidenziarsi che il Regolamento UE 2016/679 prevede che le attività di controllo del lavoratore siano svolte in un contesto di trasparenza e di adeguata protezione dei dati personali.

OBBLIGHI RELATIVI AL TRATTAMENTO DEI DATI PERSONALI	MODALITÀ DI ATTUAZIONE DEGLI OBBLIGHI SULLE ATTIVITÀ DI CONTROLLO DEL LAVORATORE
I dati devono essere trattati in modo lecito e corretto	I dati devono essere trattati in modo lecito, corretto e trasparente nel rispetto dei diritti del soggetto interessato. Le finalità devono essere determinate, esplicite e legittime. I dati trattati devono essere adeguati, pertinenti, esatti e aggiornati, oltre che limitati a quanto necessario coerentemente con le finalità del trattamento e, in ogni caso, garantendone un adeguato livello di sicurezza.
	Il Datore di lavoro/Titolare del trattamento dovrà – propedeuticamente – fornire al dipendente/soggetto interessato l'informativa che descrive il flusso del trattamento dei suoi dati. Il documento di informativa dovrà necessariamente indicare il periodo di conservazione dei dati personali, ovvero i criteri utilizzati per determinare tale periodo. Il linguaggio dell'informativa deve

Informativa all'interessato	essere semplice e chiaro. L'art. 13 del GDPR si riferisce alla fattispecie in cui la comunicazione delle informazioni sia collegata alla raccolta dei dati presso l'interessato, mentre l'art. 14 si riferisce alla fattispecie in cui la raccolta dei dati avvenga presso un soggetto terzo[44].
Trasparenza nella gestione dei trattamenti	Il titolare del trattamento è obbligato ad adottare misure adeguate al fine di fornire all'interessato tutte le informazioni/comunicazioni relative ai trattamenti gestiti dalla propria organizzazione, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. Il titolare è, altresì, obbligato ad agevolare l'esercizio di tali diritti da parte dell'interessato e, in particolare, a fornire un riscontro alla richiesta del medesimo senza ingiustificato ritardo e comunque entro un mese dal ricevimento della medesima (prorogabile di due mesi ove necessario, tenuto conto della complessità e del numero delle richieste).
Privacy by default (per impostazione predefinita	Alla base dei suddetti obblighi del titolare del trattamento vi è quello di predisporre le misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ciascuna finalità del trattamento. Obbligo che vale per la quantità dei dati raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità ai dati stessi.

In ordine alle modalità di attuazione, l'art. 88 del GDPR stabilisce che gli Stati possono emanare norme specifiche per garantire la protezione dei diritti e delle libertà dei dipendenti nell'ambito del trattamento dei dati personali che venga effettuato nel contesto del rapporto di lavoro.

[44] *"Il legislatore al comma 3* [dell'art. 4, l. n. 300 del 1970 (st. lav.)]*, nel prevedere a carico del datore di lavoro l'obbligo di fornire al suo dipendente 'adeguata informazione' sulle modalità d'uso degli strumenti tecnologici e sulle modalità di effettuazione dei controlli attraverso tali strumenti, introduce implicitamente il divieto di controlli occulti sulla prestazione lavorativa. L'informativa, tuttavia, non deve ridursi ad un adempimento formale rivolto alla generalità dei lavoratori, ma deve essere esaustiva e adeguata e tale non può essere considerata l'indicazione di istruzioni relative all'uso dello strumento tecnologico, non accompagnate dalla specifica individuazione delle modalità di utilizzo che comportano l'acquisizione dei dati".* Fonte: *Il giuslavorista.it* 15 ottobre 2018 (nota di: Apa Sabrina).

Sul piano giuslavoristico, il Legislatore nazionale aveva già emanato il **D. Lgs n. 151 del 14 settembre del 2015 (***Jobs Act*) che, di fatto, ha riscritto l'art. 4 dello Statuto dei Lavoratori[45].

Il *Jobs Act* – successivamente modificato per effetto del **D.Lgs. 185 del 2016** – stabilisce regole differenti a seconda del tipo di strumento utilizzato dal datore di lavoro per effettuare tale controllo.

DISCIPLINA GIUSLAVORISTICA DEI CONTROLLI DEL DATORE DI LAVORO	
Strumenti che consentono il controllo del lavoratore **(es. videosorveglianza)**	L'installazione di impianti audiovisivi e altri strumenti dai quali deriva anche la possibilità di controllo a distanza dell'attività dei lavoratori è di norma vietata, a meno che non ricorrano due condizioni: - esigenze organizzative e produttive, di sicurezza del lavoro e tutela del patrimonio aziendale; - preventivo accordo sindacale o, in mancanza, autorizzazione amministrativa (Direzione territoriale del lavoro). Attenzione: l'accordo sindacale o l'autorizzazione amministrativa deve precedere l'installazione dell'impianto, non solo la messa in funzione (Cass. Penale n. 4331/2014), per cui se l'impianto è installato prima dell'accordo si configura la violazione delle norme (art. 38 L. 300/1970), anche nel caso in cui i dipendenti siano stati correttamente informati. Inoltre, tale divieto di installazione di telecamere in assenza di accordo vale anche per le telecamere "finte", montate al solo scopo dissuasivo e che non registrano dati.
Strumenti di lavoro (personal computer, *smartphone*)	Ai sensi del secondo comma dell'articolo 4, le suddette garanzie non si applicano agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa (es. *smartphone, tablet, personal computer*) nè agli strumenti di registrazione degli accessi e delle presenze. L'installazione di sistemi di controllo, in tali casi, non richiede alcun accordo sindacale né autorizzazione. Si tratta di una eccezione limitata agli strumenti che *"immediatamente servono al lavoratore per adempiere alle mansioni assegnate"*. Il Ministero del Lavoro, con nota del 18 giugno 2015, ha stabilito che nel momento in cui lo strumento viene modificato (ad esempio, con l'aggiunta di *software* di localizzazione), non si considera più rientrante nella categoria. Attenzione perché: il GPS eventualmente installato su auto aziendale potrebbe "servire" al lavoratore per adempiere alle mansioni assegnate ma, al tempo stesso, potrebbe essere utilizzato dal datore di lavoro per controllare il lavoratore. Il successivo comma 3 chiarisce che le informazioni raccolte tramite gli strumenti di cui al comma 1 e 2, sono utilizzabili a tutti i

[45] L'art.4 dello Statuto dei Lavoratori, nella sua originaria formulazione, prevedeva il divieto assoluto dell'uso di impianti audiovisivi e altre apparecchiature per finalità di controllo a distanza del lavoratore. Il Legislatore aveva previsto che l'istallazione fosse permessa solo per "esigenze organizzative e produttive" e per "ragioni di sicurezza" previo accordo con le rappresentanze sindacali aziendali oppure, in mancanza di queste, con la commissione interna. In mancanza di un accordo con le rappresentanze sindacali, restava al datore di lavoro la possibilità di fare istanza all'Ispettorato del Lavoro.

	fini connessi al rapporto di lavoro a condizione che al lavoratore sia data adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli. Per "fini" si intendono anche i fini tipicamente disciplinari. Sul punto si è espresso anche il Ministero del Lavoro chiarendo che, per il principio di trasparenza, i lavoratori devono essere informati dell'esistenza e delle modalità d'uso degli strumenti di controllo, con riferimento alla finalità e alle modalità del trattamento dei dati, alla natura obbligatoria e facoltativa del conferimento dei dati, alle conseguenze di un eventuale rifiuto, ai soggetti ai quali i dati possono essere comunicati nonché ai responsabili aziendali del trattamento dei dati, oltre che dei diritti dei lavoratori. In caso di mancata informazione i dati così raccolti non potranno essere utilizzati a nessun fine[46].
Il comma 2 dell'art. 4 Statuto Lavoratori sancisce l'obbligo, a carico del datore di lavoro, di consegnare un'informativa che comunichi agli lavoratori dipendenti/soggetti interessati il funzionamento degli strumenti di lavoro nonché le collegate modalità di controllo. Tale documento di informativa deve rispettare i requisiti previsti dall'art. 13 del GDPR. Particolare risalto dovrà attribuirsi all'indicazione all'interessato di poter adire direttamente all'Autorità di controllo per eventuali segnalazioni; la finalità e la durata del trattamento dei dati; indicazione di tutti gli incaricati e responsabili del trattamento preposti al trattamento dei dati raccolti dal datore di lavoro – titolare del trattamento – infine, l'indicazione che i dati saranno trasferiti verso Paesi extra-UE.	

Sul piano della normativa privacy, è utile evidenziare che le Linee-guida 3/2019 sulla videosorveglianza varate dall'EDPB disegnano il perimetro all'interno del quale applicare il GDPR, ovvero, al trattamento dei dati personali che preveda l'utilizzo di dispositivi video. Le linee guida chiariscono, innanzitutto, che i dispositivi video che assumono rilevanza sono sia quelli più tradizionali, che quelli cosiddetti "intelligenti". Rispetto a questi ultimi dispositivi di ultima generazione, in considerazione del loro carattere più "intrusivo", le linee guida pongono particolare attenzione verso le norme relative al trattamento di particolari categorie di dati, pretendendo da titolari e responsabili dei sistemi di videosorveglianza il rispetto di un grado minimo di affidabilità, per evitare che scelte giuridiche affidate ad algoritmi, come l'identificazione facciale o il riconoscimento, possano generare effetti dannosi.[47]

La opportuna conoscenza e la corretta applicazione di quanto l'EDPB ha stabilito nelle Linee guida 3/2019 consente ai titolari e responsabili del trattamento di non rischiare che la acquisizione di video registrazioni, quand'anche legittima, non generi un trattamento illecito di quei dati o, comunque, non

[46] In materia, si segnala il Provvedimento del Garante privacy "Trattamento di dati personali dei dipendenti effettuato attraverso la localizzazione di dispositivi smartphone. Verifica preliminare richiesta da Ericsson Telecomunicazioni s.p.a. - 11 settembre 201" in Registro dei provvedimenti
n. 401 dell´11 settembre 2014, consultabile al seguente link:
https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3474069

[47] Le linee guida 3/2019 dell'EDPB riguardano, anche: la liceità del trattamento; l'applicabilità dei criteri di esclusione relativi ai trattamenti in ambito domestico e il delicato tema della divulgazione di filmati a terzi.

conforme al Regolamento generale. Il testo illustra anche i casi in cui il GDPR non si deve applicare, fornendo una serie di esempi tra i quali spicca il caso – anche questo inflazionato - delle telecamere finte[48].

Proprio un esempio pratico potrà risultare utile a chiarire i rischi che scaturiscono dall'adozione di un sistema di videosorveglianza. Se pensiamo a uno studio professionale o a un'azienda che abbia collocato al suo ingresso e all'interno dei locali un sistema di videosorveglianza.

In ragione di ciò – in linea di massima – si configurerebbe un'azione di monitoraggio sistematico su larga scala di un'area accessibile al pubblico, pertanto, ai sensi dell'art. 35, paragrafo 3, lettera c) del GDPR, scatterebbe l'obbligo della DPIA[49] e, di conseguenza, quello di provvedere alla nomina del DPO, *ex* art. 37, paragrafo 1, lettera b) GDPR[50].

Alla luce di quanto sin qui evidenziato, è possibile trarre le conclusioni di ordine operativo e schematizzare, nella seguente tabella riepilogativa, la serie di adempimenti propedeutici all'installazione di un sistema di videosorveglianza in ambiente lavorativo.

ADEMPIMENTI CHE IL LEGALE RAPPRESENTANTE DI UN'IMPRESA DEVE RISPETTARE PRIMA DI POTER INSTALLARE UN IMPIANTO DI VIDEOSORVEGLIANZA IN AMBIENTE DI LAVORO:
• Richiedere e ottenere l'autorizzazione all'installazione di impianti audiovisivi.
• Posizionare correttamente le telecamere nelle zone in cui si ritiene necessaria la sorveglianza, evitando di riprendere in maniera unidirezionale i lavoratori
• Comunicare la presenza di un sistema di videosorveglianza con cartelli ben visibili al personale, i clienti e i visitatori
• Informare i lavoratori fornendo un apposito documento di informativa sulla privacy

[48] Tra i più interessanti esempi presenti nelle linee guida dell'EDPB si segnalano, oltre a quello menzionato delle telecamere finte, che non effettuando alcuna ripresa non trattano dati personali;, quello delle video registrazioni ad alta quota e quello delle videocamera a bassa risoluzione, in entrambi gli ultimi due casi le immagini non sono riconducibili a un soggetto preciso e non ne consentono l'identificazione.

[49] Della *Data Protection Impact Assessment* (DPIA) - in italiano Valutazione di Impatto sulla Protezione dei Dati – si tratterà nel successivo Capitolo 4.

[50] L'esempio intende porre all'attenzione del lettore la portata delle ricadute che l'installazione di un sistema di videosorveglianza è idoneo a generare. Resta inteso che ciascuna singola situazione reale necessità di una specifica analisi di contesto, al fine di verificare i concreti termini di applicazione del GDPR. Con ciò si vuol porre l'attenzione sul fatto che non sempre l'installazione di un sistema di videosorveglianza genera le conseguenze ipotizzate (a titolo di esempio) tant'è che – per esempio – il GDPR non si applica negli stessi termini ipotizzati nel caso in cui le persone riprese dal sistema video – magari a bassa risoluzione - non siano in alcun modo identificabili, né direttamente né indirettamente.

• Nominare e assicurare la formazione di un responsabile del sistema di videosorveglianza
• Predisporre e attuare misure adeguate di sicurezza per garantire l'accesso alle immagini esclusivamente al personale autorizzato, ad eccezione del potere di accesso delle autorità competenti per fatti delittuosi e utilizzabili esclusivamente a titolo di prova giudiziale.
• Conservare le immagini per un tempo massimo di 24-48 ore
In mancanza di tali adempimenti, scatta la responsabilità penale del datore di lavoro. Le telecamere possono essere installate solo dopo aver ricevuto l'autorizzazione: la presenza dell'impianto di videosorveglianza, per quanto spento, necessita di previa approvazione.
Nota bene: gli strumenti che il dipendente utilizza per svolgere l'attività lavorativa (*smartphone, tablet*, …) sono esenti da autorizzazione e possono essere installati senza dover rispettare la suddetta procedura. I dati raccolti in modo regolare mediante strumenti di controllo a distanza possono essere utilizzati a tutti i fini connessi al rapporto di lavoro e quindi anche a fini disciplinari. Resta inteso che al lavoratore deve essere fornita informativa completa circa l'esistenza di tali strumenti e la modalità di utilizzo.
Le attività ispettive puntano a verificare che le modalità di utilizzo degli strumenti di controllo siano assolutamente conformi e coerenti con le finalità dichiarate.

È necessario, inoltre, che **il datore di lavoro di uno studio professionale o di un'azienda si attenga alle istruzioni operative**, dettate dall'Ispettorato Nazionale del Lavoro che sono ripotate nella seguente tabella.

ISTRUZIONI OPERATIVE PER LA CORRETTA INSTALLAZIONE E UTILIZZAZIONE DEI SISTEMI DI VIDEOSORVEGLIANZA SUI LUOGHI DI LAVORO E DEGLI STRUMENTI DI CONTROLLO(CIRCOLARE N.5 DELL'INL – ISPETTORATO NAZIONALE DEL LAVORO - 19 FEBBRAIO 2018)	
È possibile inquadrare direttamente il lavoratore qualora sussistano ragioni organizzative e produttive alla base della domanda oltre che quelle di sicurezza sul lavoro e di tutela del patrimonio aziendale	**VERO**
Si deve allegare la planimetria dei locali in quanto indicando la posizione, l'angolo e il numero delle telecamere	**FALSO (non è più necessario)** i dati relativi alle immagini registrate vanno conservati per almeno 6 mesi
È necessario adottare il sistema con doppia chiave di accesso, fisica e logica	**FALSO (non è più necessario)** Tuttavia, l'accesso alle immagini registrate (sia se effettuato da remoto che in loco) deve essere necessariamente tracciato anche tramite apposite funzionalità che consentano la conservazione dei "log di accesso" per un congruo periodo, non

	inferiore a sei mesi.
È necessario ottenere autorizzazione all'installazione delle telecamere in zone estern e estranee alle pertinenze dell'azienda.	**FALSO (non è più necessario)**
È possibile attivare il riconoscimento biometrico.	**VERO**
Nella sezione modulistica del sito istituzionale dell'Ispettorato Nazionale del Lavoro sono disponibili i nuovi modelli dell'istanza di autorizzazione all'installazione di impianti di videosorveglianza e di sistemi di controllo a distanza diversi dalla videosorveglianza con l'esatta indicazione della documentazione necessaria da allegare alla medesima. L'istanza è soggetta all'imposta di bollo nella misura di euro 16,00, così come il provvedimento di autorizzazione rilasciato dalla sede centrale o territoriale INL. https://www.ispettorato.gov.it/it-it/strumenti-e-servizi/Modulistica/Pagine/Home-Modulistica.aspx	

3.4 Piano sanzionatorio per violazioni in materia di controlli e videosorveglianza in ambiente lavorativo

In caso di violazione dell'art. 4 le sanzioni sono previste dall'art. 38 dello Statuto dei Lavoratori, che trova piena applicazione a seguito della modifica dell'art. 171 del D.Lgs. 192/2003 operata dall'art. 15, comma 1, lettera f) del D.Lgs. 101/2018.

L'ammenda varia da € 154,00 a € 1.549,00 e **l'arresto da 15 giorni a 1 anno,** salvo che il fatto non costituisca più grave reato.

Nel caso di contravvenzione, in linea di massima, l'Ispettorato del lavoro fissa un termine per la regolarizzazione che potrà consistere nella rimozione delle telecamere o, in alternativa, nella stipula dell'accordo sindacale o nell'aver ottenuto l'autorizzazione della Direzione Territoriale del Lavoro. In tal modo sarà consentito pagare un quarto del massimo dell'ammenda stabilita per la contravvenzione commessa, nel termine di trenta giorni.

Tra le violazioni all'art. 4 dello Statuto dei lavoratori, quelle caratterizzate da maggiore gravità non prevedono l'applicazione della sanzione pecuniaria bensì l'ammenda e – in alcuni casi - l'arresto, in tali casi l'Ispettorato del lavoro dovrà comunicare la notizia di reato alla Procura. Si tratta, per esempio, dell'installazione di telecamere fisse che inquadrino esclusivamente l'attività svolta dai lavoratori ovvero i luoghi adibiti esclusivamente al godimento della pausa e/o alla consumazione del pasto da parte degli stessi.

Si consiglia – ai datori di lavoro e titolari di studio professionale - di tenere in considerazione che **chiedere l'autorizzazione della DTL in un momento successivo a quello in cui sono state installate** le telecamere (seppure non ancora attivate) **espone all'applicazione della sanzione**, dato che l'ispettore della DTL in sede di sopralluogo pre-autorizzazione dovrà procedere alla contestazione. È ciò che emerge da quanto stabilito dal Ministero del Lavoro, con nota n. 11241 del 1° giugno 2016, ovvero che si ritiene violato l'art. 4 dello Statuto dei lavoratori anche nei casi in cui risulti installato un sistema di videosorveglianza che non sia attivato, essendo la condotta criminosa rappresentata dalla mera installazione non autorizzata dell'impianto, perciò a prescindere dal suo effettivo utilizzo[51].

Si deve fare attenzione, altresì, al fatto che in caso di mancata attuazione degli adempimenti previsti per la videosorveglianza, il carico sanzionatorio dell'Ispettorato del Lavoro per l'assenza di accordo sindacale/autorizzazione della DTL, viene incrementato delle sanzioni previste dal Regolamento UE 2016/679 per la violazione della protezione dei dati personali. Nel caso specifico, troverà sicura configurazione la **sanzione amministrativa pecuniaria fino ad Euro 10.000.000,00** per la mancata comunicazione ai soggetti interessati/lavoratori dell'informativa relativa al trattamento dei loro dati personali che si innesca come conseguenza dell'utilizzo di un sistema di videosorveglianza.

[51] Così: Cass. pen. n. 4331/2014, *"l'idoneità degli impianti a ledere il bene giuridico protetto, cioè il diritto alla riservatezza dei lavoratori, necessaria affinché il reato sussista* […] *è sufficiente anche se l'impianto non è messo in funzione, poiché, configurandosi come un reato di pericolo, la norma sanziona a priori l'installazione, prescindendo dal suo utilizzo o meno"*.

4.

La valutazione d'impatto per la protezione dei dati

(Dott. Giuseppe Miceli)

4.1 *Data Protection Impact Assessment*: obbligo di (auto)valutazione preventiva del rischio privacy

Nei casi in cui il trattamento di dati personali dovesse comportare un rischio[52] elevato per i diritti e le libertà delle persone interessate[53], ciò può avvenire a causa del monitoraggio sistematico[54] dei loro comportamenti o per il gran numero dei soggetti interessati di cui sono magari trattati dati sensibili o, anche, per una combinazione di questi e altri fattori, ecco che il Regolamento Ue 2016/679 pone

[52] Per rischio deve intendersi *"uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità", mentre la gestione dello stesso è da identificare nelle "attività finalizzate a guidare e monitorare un ente o organismo nei riguardi di tale rischio". Così Linee-guida concernenti la valutazione d'impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del Regolamento 2016/679"* del Gruppo di lavoro "Articolo 29", Linee guida dei Garanti europei (gruppo ex art. 29) del 4 aprile 2017, come modificate e adottate il 4 ottobre 2017 e fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018. In: *www.garanteprivacy.it*, p. 5.

[53] I diritti e le libertà ai quali potrebbe essere cagionato danno derivante da un trattamento rischioso sono quelli riconducibili alla privacy e al diritto alla protezione dei dati personali. Allo stesso modo i rischi possono concernere altri diritti fondamentali, quali la libertà di espressione e di pensiero, la libertà di movimento, il divieto di discriminazioni, il diritto alla libertà di coscienza e di religione.

[54] Si riporta, di seguito, il chiarimento interpretativo presente sul sito istituzionale del Garante privacy. Si evidenzia come le espressioni trattamenti "sistematici" e "non occasionali" indicate nell'Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione di impatto di cui ai punti 6, 11 e 12 sono riconducibili al criterio della "larga scala" così come espressamente illustrato al quinto criterio del WP 248 (pag. 11):

"5. trattamento di dati su larga scala: il Regolamento generale sulla protezione dei dati non definisce la nozione di "su larga scala", tuttavia fornisce un orientamento in merito al considerando 91. A ogni modo, il WP29 raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala: a. il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; b. il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; c. la durata, ovvero la persistenza, dell'attività di trattamento; d. la portata geografica dell'attività di trattamento;"

Si evidenzia inoltre che il termine "dati biometrici" di cui al punto 11 dell'Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione di impatto va inteso come *"dati biometrici, trattati per identificare univocamente una persona fisica"*.

l'obbligo in capo ai Titolari del trattamento di effettuare una preventiva Valutazione di Impatto sulla Protezione dei Dati personali (*Data Protection Impact Assessment*, d'ora in poi "DPIA")[55].

La valutazione di impatto sulla protezione dei dati, prevista dall'art. 35 GDPR[56], costituisce uno degli elementi di maggiore rilevanza nel rinnovato quadro normativo, in quanto espressione concreta del principio di responsabilizzazione (*accountability*) nonché dei principi di *privacy by design e by default* che il Legislatore europeo ha posto alla base del Regolamento e che devono connotare i trattamenti di dati personali operati dai Titolari (e responsabili) del trattamento[57].

Come si è già avuto modo di rilevare, lo svolgimento di un'attività di valutazione o di autovalutazione d'impatto[58] del "rischio privacy" costituisce un'operazione particolarmente complessa, tant'è che lo stesso Regolamento generale prevede la possibilità di chiedere una consultazione preventiva all'Autorità Garante per la Protezione dei Dati Personali[59], nei casi in cui le misure tecniche e organizzative individuate per mitigare l´impatto del trattamento non dovessero ritenersi sufficienti, cioè, quando il rischio residuale per i diritti e le libertà degli interessati dovesse restare elevato[60].

L'esito positivo della DPIA, ossia nei casi in cui non vi sia un rischio "residuo" elevato – bensì, accettabile - legittima, invece, il titolare a eseguire il trattamento.

[55] Nei casi in cui un trattamento sia svolto in contitolarità, nella DPIA devono essere specificati con precisione gli obblighi che incombono su ciascun titolare, ad esempio con preciso riferimento in ordine alla responsabilità delle singole misure finalizzate alla gestione dei rischi.

[56] Ai sensi dell'art. 35 par. 1: *"Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali".*

[57] L'obbligo di effettuare la DPIA è a carico del titolare del trattamento, il quale, di fatto, può rivolgersi a un consulente esperto privacy che potrà materialmente svolgere tale attività.

[58] Una violazione dei dati personali potrebbe avere sugli interessati, ad esempio, i seguenti tipi di impatto:

- impatto finanziario (dati di accesso a conti correnti, credenziali carte di credito);
- impatto reputazionale, compromissione di opportunità di lavoro (divulgazione di dati concernenti attività non ben viste nella società, come contenuti per adulti, vita sessuale, ecc...);
- furto di identità (malintenzionati che si fingono altri soggetti per perpetrare reati).

[59] Cfr. il Considerando 84 del GDPR 2016/679.

[60] Art. 36, paragrafo 1) GDPR 2016/679.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Scheda aggiornata in base alla versione delle Linee guida del WP29 emendata e adottata il 4 ottobre 2017

Valutazione di impatto sulla protezione dei dati (DPIA) – Art. 35 del Regolamento UE/2016/679

COSA È?

È una procedura prevista dall'**articolo 35 del Regolamento UE/2016/679 (RGDP)** che mira a descrivere un trattamento di dati per **valutarne la necessità e la proporzionalità nonché i relativi rischi**, allo scopo di approntare misure idonee ad affrontarli. Una DPIA **può riguardare un singolo trattamento oppure più trattamenti** che presentano **analogie** in termini di natura, ambito, contesto, finalità e rischi.

PERCHÉ?

La DPIA è uno strumento importante in termini di responsabilizzazione *(accountability)* in quanto aiuta il titolare non soltanto a rispettare le prescrizioni del RGPD, ma anche ad attestare di aver adottato misure idonee a garantire il rispetto di tali prescrizioni. In altri termini, **la DPIA è una procedura che permette di valutare e dimostrare la conformità con le norme in materia di protezione dei dati personali.** Vista la sua utilità, il Gruppo Art. 29 suggerisce di valutarne l'impiego **per tutti i trattamenti**, e **non solo** nei casi in cui il Regolamento la prescrive come obbligatoria.

IN CHE MOMENTO?

La DPIA deve essere condotta **prima** di procedere al trattamento. Dovrebbe comunque essere previsto un **riesame continuo** della DPIA, **ripetendo la valutazione a intervalli regolari.**

CHI?

La **responsabilità** della DPIA spetta al **titolare**, anche se la conduzione materiale della valutazione di impatto può essere affidata a un altro soggetto, interno o esterno all'organizzazione. Il titolare **ne monitora** lo svolgimento **consultandosi** con il **responsabile della protezione dei dati** (RPD, in inglese DPO) e acquisendo - se i trattamenti lo richiedono - il parere di esperti di settore, del **responsabile della sicurezza dei sistemi informativi** *(Chief Information Security Officer, CISO)* e **del responsabile IT.**

QUANDO LA DPIA E' OBBLIGATORIA?

In tutti i casi in cui un trattamento può presentare un **rischio elevato per i diritti e le libertà** delle persone fisiche.
Il Gruppo Art. 29 individua alcuni criteri specifici a questo proposito:
- trattamenti valutativi o di *scoring*, compresa la profilazione;
- decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni);
- monitoraggio sistematico (es: videosorveglianza);
- trattamento di dati sensibili, giudiziari o di natura estremamente personale (es: informazioni sulle opinioni politiche);
- trattamenti di dati personali su larga scala;
- combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data);
- dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, device IoT, ecc.);
- trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).

La DPIA è necessaria in presenza di almeno due di questi criteri, ma - tenendo conto delle circostanze - il titolare può decidere di condurre una DPIA anche se ricorre uno solo dei criteri di cui sopra.

QUANDO LA DPIA NON E' OBBLIGATORIA?

Secondo le Linee guida del Gruppo Art. 29, la DPIA **NON è necessaria** per i trattamenti che:
- non presentano rischio elevato per diritti e libertà delle persone fisiche;
- hanno natura, ambito, contesto e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA;
- sono stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio 2018 e le cui condizioni (es: oggetto, finalità, ecc.) non hanno subito modifiche;
- sono compresi nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA;
- fanno riferimento a norme e regolamenti, Ue o di uno stato membro, per la cui definizione è stata condotta una DPIA.

La scheda ha un mero valore illustrativo ed è in continuo aggiornamento in base all'evoluzione delle indicazioni applicative del Regolamento. Per un quadro completo: www.garanteprivacy.it/regolamentoue

Una volta adita, l'Autorità garante esprime un parere nel termine di otto settimane – termine prorogabile di ulteriore sei settimane nei casi di particolare complessità – evidenziando le misure e gli accorgimenti ulteriori che necessitano di essere implementati, oppure ammonendo il titolare o, *extrema ratio*, vietando il trattamento in questione.

L'Autorità garante, inoltre, è chiamata in causa ogni qualvolta il diritto domestico degli Stati membri prescriva che i titolari del trattamento debbano consultarla chiedendo l'autorizzazione preliminare, in ordine al trattamento da parte del Titolare del trattamento per l'esecuzione di un compito di interesse pubblico, tra cui il trattamento relativo alla protezione sociale e alla sanità pubblica[61].

La possibilità di beneficiare di una consultazione preventiva da parte del Garante privacy conferma che l'elenco[62] di cui all'art. 35 del GDPR paragrafo terzo, in cui sono riportati i casi di obbligatorietà della valutazione d'impatto, è da ritenersi meramente esemplificativo, tanto che lo stesso Garante per la protezione dei dati personali predispone periodicamente una aggiornata casistica[63]. Ciò che emerge, pertanto, è la volontà del Legislatore comunitario di incentivare una più ampia propensione alla valutazione del rischio (*risk-assessment*) e, successivamente, alla gestione dello stesso (*risk-management*), per garantire, così, la protezione delle persone fisiche.

CASI DI OBBLIGATORIETÀ DELLA DPIA E CASISTICA (NON ESAUSTIVA) DI RISCHIO ELEVATO	
La valutazione d'impatto sulla protezione dei dati è obbligatoria soltanto qualora il trattamento *"possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche"* (art. 35, paragrafo 1, 3 e 4). La valutazione d'impatto sulla protezione dei dati	– una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche; – il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne

[61] Così: ultimo paragrafo dell'art. 36 GDPR 2016/679.

[62] https://www.garanteprivacy.it/documents/10160/0/ALLEGATO+1+Elenco+delle+tipologie+di+trattamenti+soggetti+al+meccanismo+di+coerenza+da+sottoporre+a+valutazione+di+impatto.pdf/b9ceefa9-dd65-df86-fed4-df3c3570f59d?version=1.11

[63] Cfr: Provvedimento n. 467 dell'11 ottobre 2018 (pubblicato sulla G.U. n. 269 del 19 novembre 2018) del Garante per la protezione dei dati personali che ha previsto, ai sensi dell'art. 35 comma 4 del Regolamento UE n. 2016/679, l'elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati.

può essere richiesta anche in altre circostanze. L'art. 35, paragrafo 3, fornisce alcuni esempi, non esaustivi, di casi nei quali un trattamento "possa presentare rischi elevati"	penali e a reati di cui all'articolo 10; – la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

I 9 CRITERI ENUNCIATI DAL *WP ART. 29*	
La linea guida WP248 offre alcuni spunti e criteri di valutazione da tenere in considerazione al fine di valutare la necessità o meno di effettuare una DPIA di un trattamento. Le indicazioni prevedono che nel caso in cui un trattamento ricada in almeno due delle seguenti categorie si renda necessario lo sviluppo di un processo di valutazione di impatto:	1. Valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato"
	2. processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente: trattamento che mira a consentire l'adozione di decisioni in merito agli interessati che "hanno effetti giuridici" o che "incidono in modo analogo significativamente su dette persone fisiche";
	3. monitoraggio sistematico: trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o "la sorveglianza sistematica su larga scala di una zona accessibile al pubblico";
	4. dati sensibili o dati aventi carattere altamente personale: questo criterio include categorie particolari di dati personali così come definite all'articolo 9 (ad esempio informazioni sulle opinioni politiche delle persone), nonché dati personali relativi a condanne penali o reati di cui all'articolo 10.
	5. trattamento di dati su larga scala: il Regolamento generale sulla protezione dei dati non definisce la nozione di "su larga scala", tuttavia fornisce un orientamento in merito al considerando 91. A ogni modo, il WP29 raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala: • il numero di soggetti interessati dal

	trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; • il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; • la durata, ovvero la persistenza, dell'attività di trattamento; • la portata geografica dell'attività di trattamento;
	6. creazione di corrispondenze o combinazione di insiemi di dati, ad esempio a partire da dati derivanti da due o più operazioni di trattamento svolte per finalità diverse e/o da titolari del trattamento diversi secondo una modalità che va oltre le ragionevoli aspettative dell'interessato;
	7. dati relativi a interessati vulnerabili (considerando 75): il trattamento di questo tipo di dati è un criterio a causa dell'aumento dello squilibrio di potere tra gli interessati e il titolare del trattamento, aspetto questo che fa sì che le persone possono non essere in grado di acconsentire od opporsi al trattamento dei loro dati o di esercitare i propri diritti.
	8. uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative, quali la combinazione dell'uso dell'impronta digitale e del riconoscimento facciale per un miglior controllo degli accessi fisici, ecc.;
	9. quando il trattamento in sé "impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto" (articolo 22 e considerando 91). Ciò include i trattamenti che mirano a consentire, modificare o rifiutare l'accesso degli interessati a un servizio oppure la stipula di un contratto.

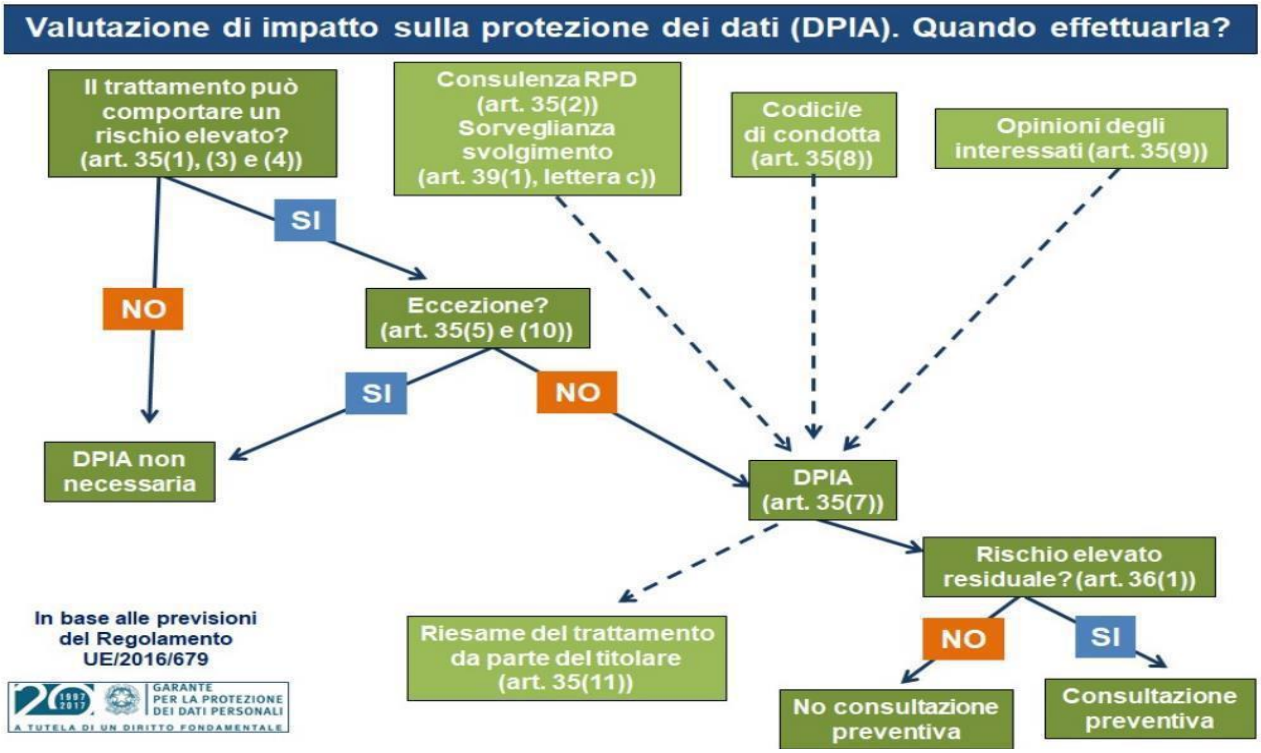
Attenzione:

Quando ricorrono almeno due dei criteri sopra indicati, il titolare dovrà condurre una DPIA. Tuttavia, il titolare del trattamento può ritenere che un trattamento che soddisfi soltanto uno di questi criteri richieda una valutazione d'impatto sulla protezione dei dati.

Di contro, pur in presenza dei criteri summenzionati, il titolare potrà ritenere di non dover svolgere una DPIA se dovesse ritenere che il trattamento non presenti un rischio elevato. In tal caso, il titolare dovrà motivare e documentare la scelta della mancata conduzione della DPIA, allegando o annotando il parere

del DPO.

L'Autorità di controllo può redigere inoltre un elenco di trattamenti per i quali la DPIA è obbligatoria. Si tratta di un elenco pubblico comunicato al Comitato Europeo per la Protezione dei Dati.



QUANDO SI PUÒ <u>NON</u> EFFETTUARE UNA DPIA	
	– trattamento che non "*presenta[…] un rischio elevato per i diritti e le libertà delle persone fisiche*" (articolo 35, paragrafo 1);
	– la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili a quelle di un trattamento analogo e per il quale è stata svolta una DPIA, tanto che si possono utilizzare i risultati di quella DPIA (articolo 35, paragrafo 11);
	– le tipologie di trattamento sono state verificate da un'Autorità di controllo prima del maggio 2018 e condizioni specifiche non sono variate;
	– trattamento che ricade nella fattispecie di deroga di cui all'articolo 35, paragrafo 10)

Casi in cui è possibile non effettuare una DPIA	(salvo che uno Stato membro non abbia dichiarato che è necessario effettuare tale valutazione prima di procedere alle attività di trattamento) – il trattamento è incluso nell'elenco facoltativo (stabilito dall'Autorità di controllo) delle tipologie di trattamento per le quali non è richiesta alcuna valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 5).

CASI DI DEROGA RISPETTO ALL'OBBLIGO DI EFFETTUARE UNA DPIA	
L'art. 35, paragrafo 10, GDPR prevede che NON dovrà essere effettuata la DPIA nei seguenti casi:	– trattamento effettuato per adempiere ad un obbligo legale cui è soggetto il titolare (art. 6, paragrafo 1, lettera c); – trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare (art. 6, paragrafo 1, lettera e).

Attenzione:

In presenza dei suddetti casi è, altresì, necessario che ricorrano entrambe le condizioni sottoindicate:

(i) il trattamento deve essere specificamente disciplinato da una disposizione del diritto dell'Unione o dello Stato membro;
(ii) deve essere già stata effettuata una valutazione d'impatto generale nel contesto dell'adozione della predetta disposizione legislativa comunitaria o statale.

Lo Stato membro può, in ogni caso, disporre che sia effettuata una valutazione di impatto *ex novo* anche alla presenza delle condizioni sopra richiamate.

4.2 Oggetto della DPIA

Oggetto della DPIA può essere un singolo trattamento ovvero un insieme di trattamenti, nel caso in cui questi siano simili, si realizzerà la cd "DPIA unitaria" prevista nel considerando 92. A ben vedere il GDPR consente – per soddisfare ragioni di economicità - a più titolari di effettuare una DPIA unitaria, nel caso tali titolari decidessero di *"introdurre un'applicazione o un ambiente di trattamento comuni in un settore o segmento industriale o per un'attività trasversale ampiamente utilizzata"*.

<table>
<tr><th colspan="2">ESEMPI RELATIVI A DPIA UNITARIA</th></tr>
<tr><td rowspan="3">WP art. 29: elenco degli esempi relativi a DPIA unitaria.</td><td>diversi titolari che decidano di installare un analogo sistema di videosorveglianza;</td></tr>
<tr><td>unico titolare (operatore ferroviario) che decida di impiegare la videosorveglianza in tutte le stazioni ferroviarie di propria competenza;</td></tr>
<tr><td>fornitore di un prodotto (nella specie, produttori di contatori intelligenti) e società utilizzatrici (nella specie, società fornitrici di elettricità), che possono utilizzare, in parte, la DPIA effettuata dal produttore in cui è stato valutato l'impatto del dispositivo tecnologico in termini di protezione dei dati.</td></tr>
</table>

La valutazione d'impatto sulla protezione dei dati è, quindi, un processo finalizzato a descrivere il trattamento, valutarne la necessità e la proporzionalità e a garantire la gestione dei rischi per i diritti e le libertà delle persone fisiche che possono derivare dal trattamento di dati personali, il tutto sulla base di una preliminare analisi dei rischi e della predisposizione delle misure necessarie per eliminarli o, almeno, arginarli.

Ecco quindi che , anche il processo di valutazione d'impatto sulla protezione dei dati deve intendersi dinamico, proprio in considerazione di una continua esigenza di aggiornamento della DPIA che dovrà garantire che la protezione dei dati e della privacy sia effettivamente adeguata nel corso dell'intero ciclo di vita del trattamento, al punto da favorirne la conformità sul piano normativo.

4.3 Soggetti della DPIA

Nell'ambito dell'attività di elaborazione della DPIA, come è già emerso, possono individuarsi i soggetti che intervengono attivamente, le corrispondenti funzioni e le responsabilità di ognuno di essi:

SOGGETTO ATTIVO	PRINCIPALI ADEMPIMENTI E RESPONSABILITÀ NEL PROCESSO DI DPIA
Titolari del trattamento (o suo delegato, Responsabile del processo *Process Owner*)	– Mette a disposizione le risorse utili alla realizzazione del processo di DPIA e assicura gli adeguamenti normativi e di sicurezza che ne scaturiscono – Coordina le attività afferenti alla DPIA per i nuovi trattamenti e le attività per l'aggiornamento della DPIA – E' responsabile della raccolta delle informazioni sul trattamento per le verifiche preventive – È responsabile della verifica e della implementazione delle misure di sicurezza necessarie. – E' responsabile delle verifiche preventive di conformità del trattamento – Assicura collaborazione al DPO nell'attività di verifica preventiva sull'obbligatorietà della esecuzione di una DPIA e nella fase di richiesta al Garante per la consultazione preventiva – Segnala al DPO il nuovo trattamento e/o la modifica del profilo di rischio – Implementa la strategia nella gestione del trattamento – È responsabile della valorizzazione degli impatti e probabilità per le minacce individuate
Responsabile per la Protezione dei Dati (RPD) o *Data Protection Officer (DPO)*	– È Responsabile della verifica preventiva di obbligatorietà della DPIA – Assiste il titolare (o il suo delegato) nella definizione della strategia e nello svolgimento della DPIA – monitora lo svolgimento, verifica se la DPIA sia stata condotta correttamente e se siano conformi al GDPR. – Coadiuva il titolare (o il suo delegato) nella verifica preventiva di conformità del trattamento – È responsabile del processo di consultazione preventiva e funge da interfaccia per l'Autorità di controllo.
ICT Security Specialist	– Supporta il processo di DPIA fornendo competenze e informazioni relativamente agli aspetti tecnici e di soluzioni di sicurezza delle informazioni – Partecipa alla valorizzazione degli impatti e probabilità per le minacce ICT individuate – Supporta il processo di DPIA con riguardo

	alle esigenze di sicurezza o operative. – Fornisce le informazioni di analisi dei rischi – Coordina metodi e standard dell'analisi dei rischi informatici con l'analisi dei rischi DPIA – Partecipa alla valorizzazione degli impatti e probabilità per le minacce ICT individuate – Coordina l'implementazione delle misure di sicurezza necessarie emerse da DPIA in ambiente ICT. – Collabora con il titolare (o il suo delegato) nel processo di Consultazione Preventiva.

Con riferimento alla complessità dell'attività di valutazione e autovalutazione del rischio privacy, deve evidenziarsi che **nell'adempiere all'obbligo di effettuare la DPIA, il Titolare** del trattamento (e, parimenti, il Responsabili del trattamento[64]) **dovrà** – a parere di chi scrive, obbligatoriamente[65] - **avvalersi dell'ausilio del Responsabile della Protezione dei Dati personali (RPD o DPO)** ove eventualmente designato, il quale sorveglia sulla conduzione della stessa e, se richiesto, esprime un parere. Nel caso in cui il titolare non sia d'accordo con quanto sostenuto dal RPD, dovrà documentare il proprio dissenso. Si vuole così realizzare il principio della trasparenza e sicurezza nelle operazioni di trattamento per limitare gli effetti negativi sulle persone.

Attenzione: il Titolare del trattamento dovrà farsi assistere anche dal responsabile del trattamento, nei casi in cui ricorra un trattamento di competenza di quest'ultimo, il quale dovrà fornire le opportune informazioni in suo possesso per agevolare la redazione di una adeguata DPIA.

Proprio al contributo di competenze che il DPO dovrà mettere al servizio del titolare del trattamento che lo ha designato e nominato, fa richiamo la Circolare 31 maggio 2019 del Ministero della Giustizia *"Regolamento generale sulla protezione dei dati (Regolamento UE 2016/679) - Valutazione d'impatto sulla protezione dei dati (cd. DPIA) - Istruzioni operative e modulistica"*.

[64] Ai sensi dell'art. 4 GDPR, il responsabile del trattamento è: *"la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati per conto del titolare del trattamento"*

[65] Il parere del Responsabile della Protezione dei Dati (RPD) nei casi in cui si debba procedere a valutazione d'impatto rappresenta un adempimento necessario, stando a una attenta lettura dell'art. 35 del GDPR. Gli articoli 35 e 39 del Regolamento UE n. 679 del 2016, pertanto, devono essere interpretati nel senso che il titolare del trattamento a rischio elevato è tenuto a richiedere un parere al responsabile della protezione dei dati personali dovendo procedere a valutazione d'impatto. Più in particolare, l'art. 35, par. 2, GDPR., là dove prevede che il titolare *"si consulta"* intende richiamare il *"parere"* menzionato dall'art. 39, par. 1, lett. c), GDPR.

Si tratta di un provvedimento di fondamentale importanza, in quanto contiene le istruzioni operative e la modulistica utili ad assolvere a quello che – giustamente – può ritenersi essere il più delicato degli adempimenti privacy previsti dal Regolamento UE n. 2016/679: la Valutazione d'Impatto sulla Protezione dei Dati.

In particolare, la consultazione e l'utilizzo della modulistica inserita nella menzionata circolare ministeriale risulterà essere – persino – dirimente con riferimento al rapporto tra titolare e DPO nella fase di richiesta di parere circa l'effettiva sussistenza dei requisiti che rendono obbligatoria la DPIA.

Attenzione: Si consiglia, tanto ai titolari di trattamento quanto ai DPO, di procedere all'effettiva **formalizzazione sia del parere espresso dal DPO circa la sussistenza dell'obbligo** della DPIA, **sia del documento di Valutazione di Impatto** sulla Protezione dei Dati che ne scaturisce con indicazione delle diverse fasi in cui la stessa si articola.

Si tratta di un consiglio operativo che si potrà apprezzare specialmente in quei casi in cui il titolare dovesse decidere di discostarsi dalle indicazioni ricevute con il parere del DPO che – per intenderci - non è vincolante.

Ancora, significativo – sul piano operativo - è tenere conto di quanto stabilito con Provvedimento n. 467 dell'11 ottobre 2018 del Garante per la protezione dei dati personali con il quale l'Authority ha disciplinato, ai sensi dell'art. 35 comma 4 del Regolamento UE n. 2016/679, l'elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati.

In relazione al contenuto della DPIA, l'art. 35 al paragrafo 7 definisce quale debba essere il contenuto minimo per la corretta e conforme redazione di un DPIA.

PROVVEDIMENTO DEL GARANTE (11 OTTOBRE 2018): **ELENCO DELLE TIPOLOGIE DI TRATTAMENTI SOGGETTI AL REQUISITO DI UNA VALUTAZIONE D'IMPATTO**
1) Trattamenti valutativi o di *scoring* effettuati su larga scala, profilazione, attività predittive;
2) Trattamenti automatizzati finalizzati ad assumere decisioni che producono effetti giuridici oppure tali da incidere in modo significativo sull'interessato, come impedire l'esercizio corretto di un diritto o di avvalersi di un bene o di un servizio o di poter continuare ad essere parte di un contratto in essere (ad es. lo screening effettuato sui clienti di una banca attraverso l'utilizzo dei dati registrati in una centrale rischi);
3) Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati online o con *App*, il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione, e i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati anche per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc;

4) Trattamenti su larga scala di dati aventi carattere estremamente personale (come definiti nelle Linee Guida), compreso dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti);
5) Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti;
6) Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo);
7) Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi *wearable*, cioè indossabili quali, ad esempio, gli *smartwatch* o gli stessi *smartphone* attraverso i software di assistenza e comando vocale, ndr.); tracciamenti di prossimità come ad es. il *wi-fi tracking*, ogniqualvolta ricorra anche almeno un altro dei criteri individuati nelle Linee Guida;
8) Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche;
9) Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. pagamenti effettuati tramite tecnologia mobile);
10) Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse;
11) Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento;
12) Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.
Resta inteso che in caso di dubbi il titolare potrà rivolgersi alle Autorità di controllo per una consultazione preventiva sulla necessità o meno di effettuare la valutazione di impatto (art. 36).

4.4 Contenuto della DPIA

Di seguito uno schema che indica quale dovrà essere il contenuto minimo di una DPIA sviluppata nell'ambito delle attività che – in linea di massima – si svolgono all'interno di uno Studio professionale.

CONTENUTO DELLA DPIA	
I contenuti della DPIA ai sensi dell'art. 35, paragrafo 7, e nei considerando 84 e 90 del GDPR	**I contenuti della DPIA, sulla base delle linee guida WP248**

"una descrizione dei trattamenti previsti e delle finalità del trattamento";	La descrizione sistematica del trattamento e delle finalità (articolo 35 §7, lett. a), ovvero: – la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono presi in considerazione (considerando 90); – vengono registrati i dati personali, i destinatari e il periodo di conservazione dei dati personali; – viene fornita una descrizione funzionale del trattamento; – sono individuate le risorse sulle quali si basano i dati personali (hardware, software, reti, persone, canali cartacei o di trasmissione cartacea); – si tiene conto del rispetto dei codici di condotta approvati (articolo 35 §8);
"una valutazione della necessità e proporzionalità dei trattamenti" (articolo 35 §7, lett. b)	La descrizione della natura, dell'ambito, del contesto e degli scopi del trattamento. Verificare che siano state determinate le misure previste per garantire il rispetto del Regolamento (articolo 35 §7 lett. d) e considerando 90): • misure che contribuiscono alla proporzionalità e alla necessità del trattamento sulla base di: – finalità determinate, esplicite e legittime (articolo 5 §1 lett. b)); – liceità del trattamento (articolo 6); – dati personali adeguati, pertinenti e limitati a quanto necessario (articolo 5 §1 lett. c)); – limitazione della conservazione (articolo 5, paragrafo 1 lett. e)); • misure che contribuiscono ai diritti degli interessati: – informazioni fornite all'interessato (articoli 12, 13 e 14); – diritto di accesso e portabilità dei dati (articoli 15 e 20); – diritto di rettifica e alla cancellazione (articoli 16, 17 e 19); – diritto di opposizione e di limitazione di trattamento (articoli 18, 19 e 21); – rapporti con i responsabili del trattamento (articolo 28); – garanzie riguardanti trattamenti internazionali (capo V); – consultazione preventiva (articolo 36).
	Indicazioni sui dati personali trattati, i destinatari e il periodo

<table>
<tr><td>"una valutazione dei rischi per i diritti e le libertà degli interessati" (articolo 35 §7 lett. c)</td><td>per il quale sono conservati.

Origine, natura, particolarità e gravità dei rischi (cfr. considerando 84). Per ciascun rischio (accesso illegittimo, modifica indesiderata e scomparsa dei dati) vengono determinate dalla prospettiva degli interessati:

• si considerano le fonti di rischio (considerando 90); • sono individuati gli impatti potenziali per i diritti e le libertà degli interessati in caso di eventi che includono l'accesso illegittimo, la modifica indesiderata e la scomparsa dei dati;

• sono individuate minacce che potrebbero determinare un accesso illegittimo, una modifica indesiderata e la scomparsa dei dati;

• sono stimate la probabilità e la gravità (considerando 90);
• sono determinate le misure previste per gestire tali rischi</td></tr>
<tr><td rowspan="10">"le misure previste per: - "affrontare i rischi"; - "dimostrare la conformità al presente Regolamento" (articolo 35 §7 lett. d) e considerando 90);</td><td>• una descrizione funzionale dell'operazione di trattamento;</td></tr>
<tr><td>• la descrizione dell’asset model su cui si basano i dati personali (es. Siti, hardware, software, reti, organizzazione, ecc.);</td></tr>
<tr><td>• la valutazione della necessità e la proporzionalità del trattamento;</td></tr>
<tr><td>• la descrizione delle misure previste per conformarsi al Regolamento;</td></tr>
<tr><td>• la descrizione del modo in cui sono gestiti i rischi per i diritti e le libertà degli interessati;</td></tr>
<tr><td>• la descrizione dell’origine, della natura, della particolarità e della gravità dei rischi;</td></tr>
<tr><td>• la determinazione delle misure previste per il trattamento di tali rischi;</td></tr>
<tr><td>• la descrizione del modo in cui sono coinvolte le parti interessate;</td></tr>
<tr><td>• il parere del DPO;</td></tr>
<tr><td>• le opinioni eventualmente raccolte dagli interessati o dei loro rappresentanti.</td></tr>
</table>

4.5 Analisi dei rischi e DPIA

In considerazione della evidente complessità di un processo DPIA e della relativa fase di analisi dei rischi, il professionista potrà affidarsi alla funzione di ausilio di alcuni strumenti applicativi idonei a

mappare e calcolare il livello di rischio e gestire le fasi del processo, sin qui descritte. Si consiglia, dunque, di avvalersi di un *kit* di strumenti che potrà risultare essere composto da:

- semplici strumenti non strutturati, come i fogli di calcolo elettronici e
- un software per la gestione di un processo DPIA.

Di particolare utilità potrà risultare **l'applicativo denominato "PIA", una risorsa *open source*** elaborata e messa a disposizione dal CNIL (Autorità francese per la protezione dei dati). Anche il **Garante italiano ha approvato l'utilità di tale software** che può costituire un affidabile modello di riferimento per gli Studi professionali e per le PMI, in fase di strutturazione di una DPIA[66].

Il processo di analisi e gestioni dei rischi viene svolto in ordine alla raccolta di tutte le informazioni utili a identificare e censire il trattamento. In fase di elaborazione della DPIA si dovrà valutare la necessità e la proporzionalità del trattamento rispetto alle finalità, con lo scopo di rendere espliciti gli scopi di impiego dei dati perseguiti con il trattamento e le ragioni delle modalità adottate e gli interessi legittimi del Titolare. Ecco perché – a parere di chi scrive – si ritiene che all'interno del *kit* di strumenti utili

[66] https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

all'elaborazione della DPIA e alla gestione del rischio privacy non possa mancare **un altro prezioso strumento**, puntualmente disciplinato dal GDPR: **il Registro dei trattamenti**[67].

Benchè la tenuta del Registro dei trattamenti non sia ritenuta sempre obbligatoria[68], non può negarsi che la scelta del professionista-Titolare del trattamento (o, anche, Responsabile del trattamento) di avvalersene ha delle importanti ricadute positive, in considerazione dell'innegabile valore supporto che il Registro esplica nell'arco di tutto il processo di analisi dei rischi.

Il Registro dei trattamenti contiene, infatti, una serie di dati e di informazioni di continua utilità per il Titolare del trattamento[69], tra cui l'elenco delle contromisure di sicurezza (sia tecnologiche che organizzative) adottate come risultato dell'analisi dei rischi di carattere più generale (art. 24 e 25) nonché di quelle misure necessarie per la corretta applicazione della DPIA.

Schematicamente una corretta DPIA dovrà verificare i seguenti aspetti relativi a ogni singolo trattamento:	
Rispetto dei princìpi applicabili al trattamento dei dati personali (CAPO II del GDPR):	**Rispetto i diritti degli interessati (CAPO III del Regolamento):**
– principio di liceità, correttezza e trasparenza	– diritto di informazione

[67] Il Regolamento Europeo 2016/679 prevede, all'articolo 30, un ulteriore attività di *compliance* aziendale, in materia di dati personali: la tenuta del registro delle attività di trattamento dei dati personali. I registri sono strumenti, fondamentali per: tracciare l'esistente; per verificare la conformità al Regolamento; per divulgare informazioni, consapevolezza e condivisione interna; ancorchè misure per la pianificazione e controllo della politica della sicurezza di dati e banche di dati.

[68] Sono tenuti all'obbligo di redazione e adozione del registro solo le imprese o organizzazioni con più di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.

La violazione agli obblighi del titolare e del responsabile del trattamento previsto dall'art. 30 comporta sanzioni pecuniarie, fino 10.000.000,00 di euro, o per le imprese fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

[69] L'art. 30 del GDPR statuisce quelle che sono le informazioni minime necessarie e che non possono mancare all'interno del Registro del trattamento che deve contenere le seguenti informazioni:

- il nome e i dati di contatto del titolare del trattamento e, se presente, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
- le finalità del trattamento;
- la descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali siano stati o saranno comunicati, compresi i destinatari di paesi terzi;
- se presenti, i trasferimenti di dati personali verso paesi terzi e la loro identificazione;
- i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- una descrizione generale delle misure di sicurezza tecniche e organizzative.

– principio di limitazione della finalità	– diritto di accesso ai dati
– principio di minimizzazione dei dati	– diritto di portabilità dei dati
– principio di esattezza dei dati	– diritto di rettifica dei dati; o diritto di cancellazione dei dati ("diritto all'oblio");
– principio di limitazione della conservazione dei dati	– diritto di limitazione del trattamento;
– principio di integrità e riservatezza	– diritto di opposizione al trattamento

4.6 Metodologia pratica di analisi e realizzazione di una DPIA

Volendo sviluppare schematicamente una metodologia pratica di analisi e realizzazione di una DPIA, potremmo schematizzarne le fasi come segue:

FASI DELLA DPIA	DESCRIZIONE DELLE SINGOLE FASI
1. Definizione dell'operazione di trattamento e del contesto in cui si applicano.	È la fase in cui si procede alla descrizione del trattamento indicando: • le operazioni svolte sui dati (es. raccolta, registrazione, conservazione, ecc..) • i dati trattati e le finalità (tipologie di dati trattati e finalità del trattamento) • le metodologie e tecniche di trattamento, nonché il luogo ove avviene e dove sono ubicati i dati stessi • categorie di soggetti interessati (dipendenti, clienti, fornitori, ecc..) • destinatari dei dati (interni e/o esterni, comunicazioni e/o trasferimenti)
2. Comprensione e valutazione dell'impatto del trattamento per i diritti e le libertà degli interessati.	Si tratta della fase in cui si procede a valutare l'impatto sugli interessati, partendo dall'analisi dello stato di sicurezza del trattamento rispetto ai parametri indicati nell'articolo 32del GDPR (Riservatezza del dato, Disponibilità del dato e Integrità del dato). È evidente che tale (prima) valutazione viene realizzata a priori e, quindi, si dovrà prendere in considerazione un evento ipotetico in cui i predetti parametri non trovano (ancora) configurazione. Ciò, tuttavia, consente di attribuire un primo livello di impatto.
3. Definizione delle possibili minacce e la valutazione della probabilità di accadimento delle minacce	In questa fase potrà risultare utile e funzionale sottoporre un questionario di 20/30 domande, suddiviso in 4 aree, all'esito del quale si ottiene un risultato compreso tra una scala di valori.

4. Calcolo e valutazione del rischio generale sul trattamento	Combinando la probabilità di accadimento della minaccia e il relativo impatto, in una griglia per ottenere la stima del livello di rischio in una scala di valori.
La scala di valori potrà essere divisa in tre livelli: BASSO/MEDIO/ALTO	

Al termine di queste quattro fasi di analisi, si potranno individuare le misure di sicurezza tecniche ed organizzative che più appropriate al livello di rischio che ne è risultato.

In ordine alla metodologia per l'analisi dei rischi, si ritiene di fare ricorso al criterio derivato dalla Norma DS/ISO/IEC 29134:2017 (Annex A) e dal documento *"Privacy Impact Assessment"* della *Commission nationale de l'informatique et des libertés,* 2015, che si basa sulla correlazione fra la Gravità **(G)** di un rischio (in relazione all'ampiezza degli impatti potenziali sugli interessati, tenendo conto delle misure esistenti) e la Probabilità **(P)** di che l'evento che provoca il danno si realizzi (in relazione alle vulnerabilità dei supporti interessati e alla capacità delle fonti di rischio di sfruttarle, tenendo conto delle misure esistenti). In tal modo, l'indice di Rischio **(R)** è funzione dell'indice di Probabilità moltiplicato per l'indice di Gravità del danno:

R = f(P, G)

Il risultato segnerà il livello di priorità da attribuire alle misure che saranno adottate per ridurre il rischio ad un livello ritenuto accettabile.

I riferimenti utilizzati per una oggettiva relazione fra livelli e valori di gravità e probabilità sono i seguenti.

Gravità (G) delle conseguenze per i diritti degli interessati (G) che il verificarsi dell'evento può produrre:

- Livello 1 - Bassa: gli interessati non subiranno alcun impatto o potrebbero incontrare qualche inconveniente che supereranno senza difficoltà.
- Livello 2 - Media: gli interessati potrebbero sperimentare notevoli inconvenienti, che possono superare nonostante alcune difficoltà.
- Livello 3 - Alta: gli interessati potrebbe avere conseguenze significative, che dovrebbero essere in grado di superare, ma con difficoltà reali e significative.
- Livello 4 - Altissima: gli interessati potrebbero avere conseguenze significative, anche irrimediabili, che potrebbero non essere superate.

Probabilità (P) che possa verificarsi un evento:

- Livello 1 - Improbabile: non sembra possibile che le minacce possano concretizzarsi.
- Livello 2 - Poco probabile: sembra difficile che le minacce possano concretizzarsi.
- Livello 3 – Probabile: sembra possibile che le minacce possano concretizzarsi.
- Livello 4 – Molto probabile: sembra molto facile che le minacce possano concretizzarsi.

Livelli di Rischio associabili alle diverse possibilità che possono verificarsi incrociando i livelli definiti di Probabilità e Gravità, si possono raggruppare in 4 Classi di Priorità secondo lo schema seguente:

Scala della probabilità					
	Molto probabile	4	5	6	7
	Probabile	3	4	5	6
	Poco probabile	2	3	4	5
	Improbabile	1	2	3	4
		Bassa	Media	Alta	Altissima
	Scala della Gravità				

- **Priorità 6-7 - Livello di Rischio Elevato**: si tratta di rischi che devono essere assolutamente evitati o ridotti applicando misure di sicurezza che ne riducano la gravità e la probabilità.
- **Priorità 4-5 - Livello di Rischio Medio**: si tratta di rischi che devono essere evitati o ridotti applicando misure di sicurezza che ne riducano la gravità o la probabilità, favorendo le misure.
- **Priorità 1-3 - Livello di Rischio Basso**: si tratta di rischi accettabili anche in considerazione del fatto che, in molti casi, si tratta di rischi che scaturiscono dal trattamento di altri rischi.

CHECK-LIST DPIA		
Raccolta delle informazioni per l'analisi dei rischi	Si devono raccogliere le seguenti informazioni minime: a) Informazioni presenti all'interno dei trattamenti b) Processi aziendali su cui si basano i trattamenti c) Finalità dei dati raccolti d) Flussi informativi e) Elenco persone autorizzate all'accesso alle informazioni f)Asset di supporto dei trattamenti (applicativi, hardware, reti, ecc.)	
Valutazione dei rischi	Identificare i possibili impatti e le relative scale di riferimento comprendenti anche le scale di probabilità di accadimento. Le tipologie di impatto possono essere, ad esempio: a) Impatti derivanti da una violazione della sicurezza fisica; b) Impatti derivanti da una violazione dei dati di identificazione o attinenti l'identità personale; c) Impatti materiali (es. perdite finanziarie o al patrimonio, perdite dovute a frodi); d) Impatti morali o biologici (es. turbamento per la diffusione di una notizia riservata, compromissione di uno stato di salute, evento lesivo dei diritti umani inviolabili o dell'integrità della persona); e) Impatti sociali (es. quando intervengono conseguenze di tipo discriminatorio, perdite di autonomia).	
Valorizzazione contromisure e rischio residuo	Si deve procedere ad associare la singola minacce ad una idonea contromisura e determinare, così, il rischio effettivo che sarà confrontato con un valore di rischio accettabile precedentemente definito. Se il valore di rischio residuo risultasse superiore alla soglia di accettabilità si dovrà procedere a implementare le contromisure applicate. In seguito dovrà essere ricalcolato il valore di rischio residuo risultante dall'applicazione delle nuove contromisure.	
Valutazioni e Piano di trattamento dei rischi	L'insieme delle informazioni raccolte ed elaborate nel corso del processo di analisi dei rischi vengono formalizzate nel piano di trattamento del rischio. Dovranno essere tracciati: a) Dati e trattamenti da proteggere (asset primari) b) Valorizzazione delle vulnerabilità e minacce (Impatti e probabilità)	

	c) Contromisure di mitigazione del rischio d) Valore del rischio residuo Il piano di trattamento dei rischi concorre, insieme a tutte le altre informazioni legate alle valutazioni preliminari, alla formalizzazione dei risultati della DPIA.	
Formalizzazione dei risultati	La documentazione che si è gerenata nel corso del processo di DPIA, viene raccolta in un Report finale da cui emergerà la GDPR *Compliance*. Tale report dovrà, altresì, indicare i livelli di rischio residuo e le tempistiche di aggiornamento del DPIA.	
Consultazione preventiva	Nel caso in cui il livello di rischio residuo sia elevato e non mitigabile (con nuove misure) occorre consultare l'Autorità di controllo per chiedere un parere fornendo le evidenze dell'analisi compiuta. Ai sensi dell'art. 36 par. 3 GDPR, la consultazione preventiva deve contenere alcune informazioni fondamentali: a) ove applicabile, le rispettive responsabilità del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo imprenditoriale; b) le finalità e i mezzi del trattamento previsto; c) le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del presente Regolamento; d) ove applicabile, i dati di contatto del titolare della protezione dei dati; e) la valutazione d'impatto sulla protezione dei dati di cui all'articolo 35; f) ogni altra informazione richiesta dall'autorità di controllo. Nella richiesta di Consultazione Preventiva devono inoltre essere indicati i dati di contatto del DPO (il DPO funge da interfaccia con il Garante). Si raccomanda di trasmettere la Richiesta di Consultazione avvenga con modalità che consentano di dimostrare la data certa della stessa comunicazione (es. PEC, Raccomandata, ecc.) visto che i tempi stabiliti per lo sviluppo del processo di consultazione preventiva decorreranno a partire da tale data.	
Revisione del processo DPIA	La DPIA è un processo DINAMICO che deve essere continuamente applicato, monitorato e revisionato. La linea guida WP248 evidenzia la necessità di effettuare	

	la DPIA a intervalli periodici, con una frequenza almeno triennale, anche se non dovessero sopraggiungere cambiamenti apparenti al trattamento. È necessaria una revisione della DPIA tutte le volte che si è in presenza di mutamenti nel contesto organizzativo o sociale per il trattamento in essere.	

4.7 Sintesi del piano sanzionatorio per la violazione dell'obbligo della DPIA

Sul piano sanzionatorio, deve evidenziarsi che il mancato svolgimento della DPIA quando il trattamento è soggetto a tale valutazione (art. 35, paragrafi 1 e 3-4), lo svolgimento non corretto di una DPIA (art. 35, paragrafi 2 e 7-9) o la mancata consultazione dell'Autorità di controllo competente ove ciò sia necessario (art. 36, paragrafo 3, lettera e) possono comportare l'irrogazione di una sanzione amministrativa pecuniaria fino a un massimo di 10 milioni di Euro, ovvero – se si tratta di un'impresa – fino al 2% del fatturato mondiale totale annuo dell'esercizio finanziario precedente, se superiore.

G.D.P.R. 2016/679: SISTEMA SANZIONATORIO
FINO A € 10.000.000,00 O 2% FATTURATO TOTALE ANNUO GLOBALE IN CASO DI VIOLAZIONE DEI SEGUENTI ARTT:
8 (consenso dei minori),
10 (trattamenti che non richiedono l'identificazione degli interessati),
23 (privacy by design e privacy by default),
24 (contitolarità del trattamento),
25 (nomina rappresentante del Titolare non stabilito nell'Unione Europea),
26 (Responsabili del trattamento),
27 (istruzioni e autorità del Titolare),
28 (documentazione relativa a ciascun trattamento di dati personali),
29 (cooperazione con l'autorità di vigilanza),
30 (sicurezza del trattamento),
31 (notificazione dei data breach all'autorità),
32 (comunicazione dei data breach agli interessati),
33 (DPIA – Data Protection Impact Assessment),
34 (consultazione preventiva dell'autorità di vigilanza),

35, 36 e 37 (designazione, posizione e compiti del DPO – Data Protection Officer),
39 e 39a (processi di certificazione).
FINO A € 20.000.000,00 O FINO AL 4% DEL FATTURATO TOTALE ANNUO MONDIALE PER LE VIOLAZIONI:
– in materia di principi base del trattamento
– condizioni per il consenso, diritti degli interessati
– trasferimento di dati personali all'estero
– mancata ottemperanza a un ordine o a una limitazione temporanea o definitiva del trattamento disposti dall'autorità di vigilanza.

5.

Esercizio dei diritti dell'interessato e azioni legali

(Dott. Giuseppe Miceli[70])

5.1 I diritti dell'interessato dal Codice della privacy al GDPR.

È necessario, a parere di chi scrive, in via preliminare approfondire come il sistema dell'esercizio dei diritti in generale e dei singoli diritti in particolare, siano cambiati con l'entrata in vigore del Regolamento europeo e la conseguente parziale abrogazione del vecchio codice della privacy. Quali parti della normativa precedente con il suo vecchio impianto formalistico volto ad organizzare gli obblighi del titolare in una serie di adempimenti, siano rimasti a fianco al nuovo paradigma dell'autovalutazione e dell'azione basata sul principio di *accountability* introdotta dal Regolamento. Ai diritti dell'interessato è dedicato l'intero capo III del Regolamento, che contemporaneamente delinea anche le generalità del primo e più importante documento del nuovo impianto privacy, così come lo era del vecchio: l'informativa.

Il Regolamento infatti specifica molto più in dettaglio rispetto al Codice le caratteristiche dell'informativa, che deve avere forma concisa, trasparente, intelligibile l'interessato è facilmente accessibile, redatta con linguaggio chiaro e semplice con la previsione ulteriore di una facilità di accesso e comprensione ulteriore nel caso la stessa abbia dei minori quali destinatari. Sempre all'interno dell'informativa, il titolare dovrà necessariamente fornire i dati di contatto del responsabile della protezione dei dati, comunemente definito d.p.o. dall'acronimo inglese Data Protection Officer, la base giuridica del trattamento ed il proprio interesse legittimo, nonché informazioni ulteriori in caso di trasferimento dei dati all'estero e l'esistenza di attività di profilazione. Ma l'informativa è, senza dubbio, lo strumento con cui l'interessato viene a conoscenza dei propri diritti, garantiti erga omnes dal Regolamento. Nel momento in cui il consenso viene erogato, lungi dall'essere una semplice adesione strumentale ad esempio all'espletamento di un contratto, il legislatore europeo ha inteso fornire attraverso il sistema dei diritti dell'interessato un vero e proprio strumento di negoziazione che colmasse

[70] Il Paragrafo 5.1 è stato scritto dall'Avv. Luca Malatesta

l'asimmetria informativa tra le parti nel fondamentale momento del passaggio di mano del dato personale.

Entrando nel dettaglio, vediamo come **sia mutato l'impianto innanzitutto dell'esercizio dei diritti** stessi, le cui modalità sono previste negli articoli 11 e 12 del Regolamento. **Il termine per la risposta all'interessato viene fissato tassativamente in un mese dalla richiesta,** estendibile a 3 solo in caso di particolare complessità. L'attività svolta per dare riscontro all'interessato non è necessariamente a titolo gratuito, anzi sussiste una previsione espressa della **possibilità per il titolare di richiedere un contributo all'interessato qualora le richieste siano manifestamente infondate**, eccessive ovvero ripetitive. Il riscontro all'interessato, che deve essere comunque fornito entro un mese anche se si richiede tempo per operazioni suppletive, deve essere comunque dato in modo coinciso, trasparente e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Naturalmente l'obbligo di dare riscontro all'interessato é del titolare del trattamento che ne ha raccolto il consenso, ma resta comunque in capo al responsabile l'obbligo di coadiuvare il titolare agevolandone l'attività.

Nel novero dei diritti dell'interessato il primo, tanto logicamente che nel dettato normativo, è il **diritto di accesso normato** nell'articolo 15. Tale diritto prevede in ogni caso l'obbligo per il titolare di fornire una copia dei dati personali oggetto di trattamento, mentre non persiste l'obbligo di fornire una descrizione di dettaglio delle modalità di trattamento, inoltre sarà sempre obbligatorio informare l'interessato circa il tempo di conservazione ovvero, se ciò non è possibile, i criteri utilizzati per tale periodo. Andranno sempre indicate anche le garanzie applicate in caso di trasferimento di dati verso paesi terzi.

Successivamente, all'articolo 17, il Regolamento definisce **il diritto all'oblio** come un diritto alla cancellazione dei propri dati personali in forma rafforzata. È previsto infatti che il titolare che riceva la richiesta da parte dell'interessato di obliterare i propri dati personali, anche se abbia reso pubblico il dato in questione, ad esempio pubblicandolo su internet, di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati.

Di particolare interesse per questa nostra analisi diretta ai professionisti regolamentati, quindi anche ai giornalisti, il diritto all'oblio rappresenta uno degli aspetti in cui il GDPR ha modificato il diritto di cronaca. Il Garante infatti, sin dalla vigenza del vecchio Codice si è dovuto preoccupare delle modifiche che l'utilizzo della rete stava portando al mondo del giornalismo. Senza approfondire in questa sede la tematica di grande attualità relativa alle cosiddette *fake news*, ovvero a fenomeni come il *citizen journalism,* o giornalismo partecipato, il fenomeno che a parere di chi scrive interessa maggiormente il giornalista professionista dal punto di vista del GDPR riguarda la cosiddetta "coda di internet", ossia la capacità di una notizia obsoleta di restare facilmente accessibile e disponibile ad un'utenza

indifferenziata attraverso ad esempio il meccanismo delle copie cache di Google, per essere poi utilizzata in ricostruzioni che nulla hanno di accurato al fine di dimostrare una certa tesi. Si veda ad esempio come la notizia di una condanna penale vecchia di anni, magari ormai scontata per intero, lungi dal rimanere esclusivamente disponibile all'autorità giudiziaria ovvero da chi accede al casellario, diventa di dominio pubblico su Googl,e andando ad incidere sulla sfera privata dell'interessato anche dopo molto tempo.

Il Garante già con due provvedimenti negli anni 2012 e 2013 , stabilì che gli archivi giornalistici online dovessero essere sempre aggiornati, ordinando a un gruppo editoriale "di predisporre, nell'ambito dell'archivio storico on-line del quotidiano (…) un sistema idoneo a segnalare, ad esempio a margine dei singoli articoli o in nota agli stessi, l'esistenza di sviluppi delle notizie relative al ricorrente".

Pertanto, pur nella consapevolezza che il diritto di cronaca è considerato essenziale di pubblico interesse, il giornalista professionista dovrà necessariamente contemperare il principio contenuto nel gdpr con la limitazione del trattamento dei dati alle operazioni strettamente necessarie.

Un buon esempio di questa linea di condotta volta alla limitazione della spettacolarizzazione dell'indagine, è contenuta nel provvedimento del 23 marzo 2019 dove il Garante Privacy, a seguito della pubblicazione senza alcuna misura preventiva di oscuramento censura del volto di un uomo che, presumibilmente sotto l'effetto di stupefacenti, compiva atti autolesionistici all'interno di un commissariato di polizia, ha ritenuto di sanzionare la mancanza di rispetto della dignità e del decoro personale dell'interessato.

Ne discende un **quadro informativo profondamente mutato rispetto al vecchio Codice**. **Oggi l'interessato potrà**, opponendosi al trattamento**, esercitare il diritto all'oblio mediante la cancellazione dei propri dati** anche **dagli archivi storici e dalle pagine web** quando la notizia violi i principi di cui sopra, ovvero quando sia trascorso un adeguato lasso di tempo dall'evento tale da far venir meno il pubblico interesse posto alla base dell'esercizio del diritto di cronaca. Naturalmente **è sempre possibile ottenere che l'accesso alla notizia venga limitato**, ad esempio mediante la cosiddetta deindicizzazione, ossia la cancellazione dai motori di ricerca e, pur permanendo all'interno del sito su cui è stata pubblicata in origine. A fianco alla nuova specificazione del diritto all'oblio, permane comunque il **diritto all'aggiornamento dei dati**, ad esempio quando a seguito di un processo l'imputato risulti innocente, richiedendo ai gestori dei motori di ricerca di ripulire dai propri algoritmi le associazioni automatiche tra, ad esempio, un nome e cognome e un fatto di cronaca giudiziaria.

Il **diritto di limitazione del trattamento dei dati** previsto dall'articolo 18 del Regolamento, si inquadra in modo intermedio tra la cancellazione e la rettifica, non avendo quale presupposto una violazione dei presupposti di liceità del trattamento. In buona sostanza l'interessato ha il diritto di

richiedere il blocco di qualunque operazione in cui i propri dati vengono processati ad esclusione della conservazione. Ad esempio mentre si è in attesa di una sentenza di accertamento in sede giudiziaria, ovvero nel caso in cui una rettifica dei dati sia stata richiesta dall'interessato è rifiutata dal titolare. Il diritto alla limitazione del trattamento, come specificato dal garante prevede che il dato personale venga contrassegnato in attesa di determinazioni ulteriori, pertanto è opportuno che i titolari prevedono nei propri sistemi informativi misure idonee a tale scopo.

Il **diritto alla portabilità dei dati**, di facile connotazione per tutti noi che conosciamo la portabilità di un numero telefonico da un operatore all'altro, è forse nel pratico più di altri impatta sulla categoria dei professionisti: già ad una prima lettura non sfugge, infatti, come nella delicata fase di un passaggio di consegne durante un incarico tra un professionista e l'altro, la previsione contenuta nell'articolo 20 del Regolamento possa diventare decisamente onerosa per quello studio che debba impiegare tempo e risorse per riorganizzare archivi e database per il passaggio di consegne.

Per tale motivo il diritto alla portabilità è stato **oggetto di numerosi provvedimenti del Garante** volti ad indicare i criteri per il bilanciamento tra diritti e libertà fondamentale di terzi e quelli degli interessati che esercitano i diritti.

Si tratta in sostanza della previsione di trasmettere i dati da un titolare all'altro in formati interoperabili, normalmente intellegibili attraverso sistemi alla portata di tutti e non coperti, ad esempio da algoritmi di crittografia inaccessibili dall'altra parte che riceve i dati.

Le attuali linee guida adottate dal garante, limitano l'applicazione del diritto alla portabilità ai i dati che siano chiaramente riferibili all'interessato, quindi con l'esclusione dei dati anonimi ovvero ai dati che siano trattati sulla base del consenso preventivo dell'interessato o di un contratto di cui è parte l'interessato: sono quindi esclusi ad esempio i dati riferibili all'esercizio del diritto di cronaca di cui sopra. I dati devono essere trattati attraverso strumenti automatizzati, quindi con l'esclusione degli archivi cartacei nonché forniti consapevolmente (tanto ad esempio attraverso la compilazione di un modulo, che ad esempio utilizzando un programma che registri i dati dell'utente in modo automatico).

È importante a notare che l'esercizio del diritto alla portabilità non pregiudica nessuno degli altri diritti dell'interessato, che può ad esempio continuare a fruire del servizio anche dopo un'operazione di portabilità oppure richiedere la cancellazione dei dati.

5.2 Analisi schematica dei diritti dell'interessato

Il Capo III del GDPR recante *"Diritti dell'interessato"* individua i diritti del soggetto interessato e gli strumenti operativi cui poter fare ricorso per far valere tali diritti e per ottenere la giusta tutela nei casi in cui si ritenga che il trattamento dei propri dati personali sia stato realizzato in violazione delle disposizioni del Regolamento.

TABELLA SCHEMATICA DEI DIRITTI DELL'INTERESSATO		
DIRITTO DELL'INTERESSATO	GDPR ART.	DESCRIZIONE
Accesso ai dati	15	Il soggetto interessato ha il diritto di ottenere (gratuitamente) dal Titolare del trattamento la conferma che sia in atto – o meno – un trattamento di dati personali che lo riguarda, quindi di ottenere l'accesso a tali dati e alle informazioni su cui si basa il trattamento dei dati personali che lo riguardano. In particolare l'interessato deve avere accesso a: • finalità del trattamento; • categorie di dati personali in questione; • destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali; • quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; • esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento; • diritto di proporre reclamo a un'autorità di controllo; • qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine; • esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato; • garanzie adeguate relative al trasferimento dei dati, nel caso in cui siano trasferiti a un paese terzo o a un'organizzazione internazionale.
Rettifica dei dati	16	Il GDPR riconosce all'interessato il "potere" di mantenere il controllo costante e attivo sui propri dati e sull'utilizzo che ne viene fatto. Il diritto di rettifica consente di ottenere la correzione o modifica dei dati nel caso risultassero errati, non aggiornati o insufficienti. L'interessato può ottenere dal titolare del trattamento la correzione senza ritardo dei dati inesatti che lo riguardano. Inoltre, tenuto conto delle finalità del trattamento, l'interessato potrà ottenere l'integrazione dei propri dati incompleti, anche fornendo una dichiarazione integrativa.

Cancellazione dei dati c.d. diritto all'oblio (Introdotto *ex novo* dal GDPR)	17	L'interessato può chiedere al titolare del trattamento la cancellazione dei propri dati, il quale deve procedervi, senza ingiustificato ritardo, in tutti i casi in cui i dati personali non siano più necessari rispetto alle finalità per cui erano stati originariamente trattati, oppure siano stati trattati illecitamente, oppure l'interessato revochi il consenso o si opponga al loro trattamento, oppure la cancellazione costituisca un obbligo giuridico imposto dal diritto dell'UE o degli Stati membri. Il rifiuto della cancellazione da parte del titolare del trattamento può essere giustificato quando il trattamento sia necessario per l'esercizio del diritto alla libertà di espressione e di informazione, oppure avvenga nell'adempimento di un obbligo giuridico previsto dal diritto dell'UE, oppure sia motivato dall'interesse pubblico nel settore della sanità pubblica, oppure abbia finalità di archiviazione nel pubblico interesse, di ricerca scientifica o storica o fini statistici, oppure infine sia necessario per l'esercizio o la difesa di un diritto in sede giudiziaria.
Limitazione del trattamento (Introdotto *ex novo* dal GDPR)	18	Si tratta del diritto che consente all'interessato di pretendere, dal titolare, una limitazione dell'uso dei propri dati. Si può esercitare quando ricorre una delle seguenti ipotesi: a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali; b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo; c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria; d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.
Diritto alla portabilità dei dati (Introdotto *ex novo* dal GDPR)	20	Consente all'interessato di riutilizzare i propri dati, già oggetto di trattamento da parte di un titolare, per altri scopi. Si concretizza nel diritto di ricevere da un titolare del trattamento i propri dati personali, precedentemente forniti, in un formato strutturato, di uso comune, leggibile da dispositivo automatico e interoperabile al fine di memorizzarli su un dispositivo proprio (o nella propria disponibilità) ed, eventualmente, di trasferirli a un altro titolare indicato dall'interessato.
Diritto di opposizione (Introdotto *ex novo*	21	L'interessato può opporsi al trattamento dei dati che lo riguardano, in qualunque momento, per motivi connessi alla propria situazione particolare, a trattamenti fondati su alcune specifiche basi di legittimità, quali la necessità di eseguire compiti di interesse pubblico o connessi all'esercizio di pubblici poteri del titolare del trattamento, ovvero sul legittimo interesse

dal GDPR)		
Il titolare del trattamento è obbligato a rendere effettivo l'esercizio di questi diritti, a tal fini sarà sua cura predisporre idonei strumenti e sistemi in grado di agevolare l'accesso diretto dell'interessato alle informazioni che lo riguardano, così da permettergli di intervenire prontamente e, per quanto possibile, autonomamente per modificare dai dati inesatti. A tal fine, si consiglia di mettere a disposizione degli utenti/soggetti interessati la modulistica relativa all'esercizio di ciascuno dei diritti previsti e disciplinati dal GDPR.		

Le informazioni sul trattamento dei dati personali devono, inoltre, contenere la possibilità che il partecipante allo studio revochi il suo consenso in qualunque momento (e senza motivazioni). In questo caso è lecito il trattamento effettuato prima della revoca del consenso. Inoltre, **il consenso deve poter essere revocato con la stessa facilità con la quale è prestato**, quindi il Titolare del trattamento deve agevolare tale esercizio.

Le informazioni sul trattamento dei dati personali devono contenere il **diritto di proporre reclamo presso un'Autorità di Controllo.** Sarebbe utile inserire nelle informazioni sia i dati web e/o di contatto del Garante Privacy, sia delle altre autorità di controllo dell'Unione Europea.

Le informazioni sul trattamento dei dati personali devono specificare se la comunicazione di dati personali (ai destinatari) è un obbligo di legge o contrattuale, se il partecipante allo studio ha l'obbligo di fornire tali dati e le possibili conseguenze nel caso in cui lo stesso non volesse procedere con la comunicazione.

Infine, le informazioni devono specificare se è in atto un processo decisionale automatizzato (art. 22 del GDPR), con la logica utilizzata, l'importanza e le conseguenze di tale trattamento.

5.3 Reclami, ricorsi e azioni per il risarcimento del danno

Il Capo VIII (Mezzi di ricorso, responsabilità e sanzioni) del Regolamento 2016/679 UE tratta dei reclami e dei ricorsi giurisdizionali.

Più nello specifico, il diritto di proporre reclamo all'Autorità di controllo è previsto dall'art. 77[71]; il diritto al ricorso giurisdizionale effettivo nei confronti dell'Autorità di controllo è previsto dal successivo art. 78; il diritto al ricorso giurisdizionale effettivo nei confronti del titolare del trattamento o del responsabile del

[71] L'art. 13, c. 2, lett, d), GDPR, prevede l'obbligo di informare esplicitamente l'interessato del "*diritto di proporre reclamo ad un Autorità di controllo*".

trattamento è previsto dall'art. 79. A questi strumenti di tutela si deve aggiungere il diritto di trasmettere all'Autorità Garante le segnalazioni di cui all'art. 144 del D.Lgs. 196/2003 così come modificato dall'art. 13 del D. Lgs. 101/2018.

Il Legislatore nazionale ha imposto all'interessato un'alternativa obbligata[72] tra:

- proporre reclamo al Garante;
- adire l'Autorità giudiziaria.

Ecco quindi che, nel caso in cui l'interessato dovesse ritenere violati i diritti di cui agli artt. da 15 a 22 del GDPR (ovvero, quelli esaminati nel precedente paragrafo di questo Capitolo V) potrà proporre reclamo al Garante o, in alternativa, adire l'Autorità giurisdizionale, agendo direttamente nei confronti del titolare o del responsabile del trattamento[73].

Ai sensi dell'art. 77, comma 1, l'interessato ha il diritto di proporre un reclamo all'autorità di controllo e sancisce che: *"Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento che lo riguarda violi il presente Regolamento ha il diritto di proporre reclamo a un'autorità di controllo, segnatamente nello Stato membro in cui risiede abitualmente, lavora oppure del luogo ove si è verificata la presunta violazione".*

Ciascun paese membro UE si è, infatti, dotato di una Autorità di controllo competente a ricevere i reclami proposti a seguito di eventuali violazioni del GDPR o delle norme nazionali in materia di protezione dei dati[74].

Nel nostro caso, l'autorità di controllo nazionale è il Garante per la protezione dei dati personali, un'Autorità Amministrativa Indipendente, prevista e disciplinata dal Codice della Privacy, con il compito

[72] Nel nostro ordinamento, il reclamo si pone come alternativo all'azione giudiziaria, perciò se tra le medesime parti e per lo stesso oggetto risulta già stata avviata un'azione davanti all'Autorità giudiziaria, il reclamo al Garante non potrà essere proposto e viceversa, se è stato proposto reclamo al Garante, sarà improponibile la domanda innanzi all'Autorità Giudiziaria, salvo quanto previsto dal D. Lgs. 150/2011 (Disposizioni complementari al codice di procedura civile in materia di riduzione e semplificazione dei procedimenti civili di cognizione, ai sensi dell'articolo 54 della legge 18 giugno 2009, n. 69.) all'art.10, c. 4, del (Delle controversie in materia di applicazione delle disposizioni del codice in materia di protezione dei dati personali).

Infatti, benché il reclamo rappresenti come abbiamo visto, secondo il GDPR, lo strumento d'elezione in mano all'interessato per sollecitare l'Autorità di controllo a svolgere le opportune verifiche in casi di non conformità e a adottare i provvedimenti più idonei per far cessare le violazioni, occorre, però, ribadire che.

[73] Il Foro giurisdizionale competente è quello di stabilimento di titolare e responsabile oppure di residenza abituale dell'interessato (Art. 79 GDPR).

[74] La competenza in questo caso, è stabilita in base al luogo di residenza abituale o di lavoro dell'interessato, oppure al luogo in cui si è verificata la violazione.

di prendere in esame i reclami e le segnalazioni proposti dai soggetti interessati che lamentino la violazione della normativa in materia di protezione dei dati personali, la stessa *Authority* ha il compito di decidere sui ricorsi stessi.

Fondamentale, dunque, è individuare il significato e gli effetti del reclamo, così come previsto e disciplinato dall'art. 142 del Codice della Privacy. Si tratta di un **atto circostanziato** attraverso il quale l'interessato denuncia all'autorità garante la violazione delle disposizioni in materia di protezione dei dati personali. È bene evidenziare che l'atto di reclamo non è soggetto a formalità e, pertanto, può essere proposto **senza doversi necessariamente attenere a schemi o forme prestabilite**, tuttavia, è fondamentale che il reclamo contenga le indicazioni relative a:

- fatti e circostanze su cui si fonda il reclamo stesso;
- disposizioni che si presumono violate;
- misure richieste e
- estremi identificativi del titolare, del responsabile (se conosciuto) e dell'istante[75].

Al reclamo **dovranno essere allegati i documenti utili** per provare quanto sostenuto[76].

Lo stesso Codice al successivo art. 143 stabilisce che alla proposizione del reclamo può seguire una fase istruttoria, al termine della quale, se il reclamo non risulta manifestamente , il Garante esercita i poteri di indagine (c. 1), poteri correttivi (c. 2), poteri autorizzativi e consultivi (c. 3) di cui all'art. 58 del GDPR e se ne sussistono i presupposti, adotta un provvedimento (come, ad esempio, il blocco del trattamento o l'adozione di misure al fine di rendere il trattamento conforme alla normativa).

Invece, nell'ipotesi in cui l'Autorità non dovesse esprimere un provvedimento in relazione al reclamo presentato, senza nemmeno fornire informazioni circa l'esito dello stesso entro il periodo di tre mesi, ecco che l'interessato avrà il diritto di proporre ricorso giurisdizionale "effettivo" innanzi all'Autorità giurisdizionale dello Stato in cui l'Autorità di Controllo è stabilita (art. 78 GDPR).

L'altra circostanza in cui si può ricorre all'A.G. è: il **ricorso giurisdizionale avverso la decisione del Garante,** ai sensi degli articoli 143 e 152 del Codice e dell'articolo 78 del Regolamento.

Infine, **la segnalazione di cui all'art. 144 del Codice privacy** che è, invece, uno strumento che consente all'interessato di circostanziare in maniera più dettagliata la violazione per la quale si richiede

[75] Il Garante per la Protezione dei Dati, in esecuzione delle già menzionate norme, ha pubblicato sul proprio sito istituzionale un modello di reclamo utilizzabile: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4535524

[76] Giova evidenziare che la presentazione del un reclamo è gratuita.

l'intervento del Garante. Gli stessi citati provvedimenti di cui all'Art. 58 del GDPR, possono essere adottati dal Garante, a seguito della segnalazione, come pure d'ufficio, quindi in mancanza di un'attivazione esterna.

Focus - Attività di ispezione e impianto sanzionatorio

(Dott. Giuseppe Miceli)

a) Le ispezioni: operatività e consigli utili

Con la *newsletter* del 25 marzo 2019 Il Garante per la Privacy ha pubblicato - sul sito *www.garanteprivacy.it* - la Deliberazione del 14 febbraio 2019 relativa all'attività ispettiva effettuate dall´Ufficio nel primo semestre 2019, anche in collaborazione con il Nucleo Speciale Tutela Privacy e Frodi Tecnologiche, del Corpo della Guardia di Finanza[77].

Tale attività ispettiva è prevista e disciplinata al Capo III - *Accertamenti e controlli* - del Codice privacy, in particolare gli artt. 157 (*richiesta di informazioni e documenti*) e 158 (accertamenti) del codice privacy.

Deve tenersi conto che le attività ispettive e di controllo in materia di privacy, così come previste e disciplinate dal GDPR hanno abbandonato l'obsoleto carattere di "staticità" tipizzato in una mera spunta della c.d. *"check-list privacy"* e hanno assunto il carattere della "dinamicità" che contraddistingue la ricerca continua e pro-attiva di *compliance* rispetto al GDPR, alla normativa nazionale e ai provvedimenti delle Autorità di controllo.

In pratica: in fase di attività ispettiva potrà anche emergere la mancata adozione di una "misura" di protezione dei dati personali (per esempio, la nomina del DPO) tuttavia, non automaticamente ne scaturirà la contestazione e la sanzione.

Determinante sarà – sulla base del principio di *accountability* – la condotta del titolare del trattamento, sottoposto al controllo, che potrà dare dimostrazione (Comprovare) sulla base della ricostruzione logico-giuridica che non si tratti di un mancato adempimento, bensì del legittimo risultato di una attenta valutazione.

Dirimente, pertanto, in fase di ispezione, è la capacità del titolari o responsabile del trattamento di saper dare conto – in maniera *accountability* - delle scelte operate e delle decisioni applicate.

[77] Tale collaborazione è frutto del Protocollo d'Intesa tra Garante della Privacy e Guardia di Finanza, siglato il 10 marzo 2016 che tratta: della gestione dei rapporti con l'Autorità Garante; dell'esecuzione di ispezioni su delega dell'Autorità Garante; partecipazione a ispezioni congiunte con l'Autorità; dello sviluppo di attività progettuali in sinergia con i Reparti territoriali del Corpo della G. di F. e, infine, dell'individuazione soggetti da proporre quali destinatari delle ispezioni. In relazione a quest'ultimo aspetto, si rileva che le ispezioni vengono svolte non esclusivamente nei confronti dei soggetti nei confronti dei quali gli interessati abbiano trasmesso reclami o segnalazioni.

I poteri ispettivi del Garante consentono l'accesso a banche dati, archivi nei luoghi in cui si svolge il trattamento o nei quali è necessario effettuare verifiche utili al controllo del rispetto della normativa sul trattamento dei dati personali. Inoltre, il Garante può chiedere al titolare, al responsabile, al rappresentante del titolare o del responsabile nominati, all'interessato o anche a terzi di fornire informazioni o di esibire documenti anche in relazione a banche dati.

Ai sensi dell'art. 158, c.4, del Codice privacy, se l'ispezione disposta dal Garante deve svolgersi in una abitazione o un altro luogo di dimora privata è necessario *"l'assenso informato del titolare o del responsabile, oppure previa autorizzazione del presidente del tribunale competente per territorio in relazione al luogo dell'accertamento, il quale provvede con decreto motivato senza ritardo, al più tardi entro tre giorni dal ricevimento della richiesta del Garante quando è documentata l'indifferibilità dell'accertamento"*[78].

L'accertamento non può essere iniziato prime delle ore sette e dopo le ore venti salvo diversa disposizione del decreto del presidente del Tribunale.
In caso di rifiuto gli accertamenti sono comunque eseguiti e le spese ove occorrenti sono poste a carico del titolare con il provvedimento che definisce il procedimento.

È bene evidenziare che le ispezioni possono avvenire a sorpresa oppure, in alcuni casi, a seguito di avviso del Garante o della Guardia di Finanza che ne possono dare comunicazione tramite posta elettronica, il giorno prima del sopralluogo.
Attenzione: in alcuni casi l'impresa o lo studio professionale, in quanto titolari o responsabili del trattamento, possono ricevere la sola richieste di informazioni da parte dell'Autorità, senza l'espressa previsione di una successiva attività di ispezione. Ebbene, in tali casi il livello di esaustività delle informazioni fornite dal Titolare/Responsabile del trattamento sarà inversamente proporzionale alla probabilità che si realizzi una conseguente attività ispettiva da parte del Garante. Ciò significa che si dovrà prestare massima attenzione e solerzia nel soddisfare la richiesta di informazioni, affinchè possa dissiparsi la necessità del Garante di procedere all'ispezione.

Sul piano operativo è bene evidenziare che contestualmente alle operazioni di accesso, **gli ispettori esibiscono – oltre alle tessere di riconoscimento[79] - la "*richiesta di informazioni*"** ovvero

[78] In quest'ultimo caso dovrà essere rilasciata una copia del provvedimento di autorizzazione del Tribunale alla parte.

[79] Si ricorda che le attività ispettive sono condotte in genere dai militari del Nucleo Speciale Privacy della Guardia di Finanza che possono essere, o meno, accompagnati dai funzionari del Garante. Specularmente, in altri casi, sono i funzionari del Garante a procedere alle ispezioni con o senza il supporto dei finanzieri.

documento con il quale il Garante chiede al soggetto sottoposto a ispezione di dare conto degli obblighi – auspicabilmente – assolti, in materia di protezione dei dati personali, nonchè delle modalità di adempimento[80]. Lo stesso documento, dunque, è di fondamentale importanza, dato che individua il "perimetro" delle attività ispezione cui si inizia a dare corso.

Con il documento di richiesta di informazioni il Garante può chiedere di dare conto, per esempio: delle modalità attraverso cui gli interessati vengono portati a conoscenza dell'informativa; di come viene raccolto il consenso (se necessario); delle nomine di eventuali responsabili del trattamento (interni o esterni); delle modalità di conservazione dei dati personali e dei criteri di definizione della durata dei trattamenti stessi; delle misure di sicurezza di cui si sia dotato il titolare o responsabile del trattamento sottoposto all'attività ispettiva e in ultimo – ma non per importanza – può essere richiesto al titolare di "comprovare" di aver provveduto alla formazione obbligatoria (almeno a scadenze annuali e comunque in stretta relazione al trattamento dei dati svolto in azienda) dei dipendenti. Esibendo idonea documentazione a supporto.

N.B.: l'art. 83.4 GDPR fissa per la mancata erogazione della formazione la sanzione fino a 10 milioni di euro o, per le imprese, fino al 2 % del fatturato mondiale annuo dell'anno precedente se superiore.

Ecco quindi che proprio il momento in cui si innesca l'attività ispettiva può assumere importanza determinante rispetto all'esito della verifica.

Se è vero, come è vero, che la "*richiesta di informazioni*" è utile alla parte assoggettata al controllo, in quanto è sulla base di tale documento che si dovranno delimitare i poteri di controllo del Garante, è altrettanto vero che l'inadempimento alla richiesta di informazioni e la mancata esibizione dei documenti in essa indicati potrà comportare l'irrogazione di una sanzione pecuniaria fino a venti milioni di euro o per le imprese fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente.

[80] L'obbligo formativo è previsto dall'art. 39.1.b del GDPR, che indica tra i compiti del DPO quello di: "*sorvegliare l'osservanza* […] *delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi* […] *la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo*"; inoltre l'art. 29 e l'art. 32.4 sanciscono che *"chiunque abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento".*

Attenzione: Il consiglio più opportuno è, dunque, quello di prestare massima attenzione alla fase di presentazione degli ispettori e a quella di approccio all'attività ispettiva e di non lesinare i dovuti atti di collaborazione pro-attiva.

Restando sul piano dell'operatività, al titolare o responsabile del trattamento nei cui confronti si sta svolgendo l'ispezione, potrà risultare particolarmente utile chiedere di esercitare la facoltà di farsi assistere, già dalle prima fasi della verifica, da consulenti di fiducia (avvocato esperto in materia di privacy o consulente tecnico informatico). Mentre, invece, diamo per scontata la presenza del DPO (ove sia stato nominato) se non altro perché - come è noto – tra i suoi principali doveri vi è quello di fungere da interfaccia con l'Autorità di controllo.

Altrettanto delicata e importante è la fase in cui gli ispettori procedono – nel contraddittorio con la parte - alla **redazione del verbale di operazioni** compiute.

Si tratta della fase in cui vengono verbalizzate tutte le attività svolte e le modalità di svolgimento, a partire dall'accesso e fino alla chiusura dell'attività ispettiva o alla sua sospensione, nel caso in cui le attività dovessero interrompersi per poi riprendere il giorno seguente o dopo una interruzione dettata da altri motivi.

Il verbale - redatto a cura degli ispettori – potrà riportare eventuali dichiarazioni della parte o dei presenti alle attività di verifica (premesso che ciascun presente dovrà essere formalmente identificato tramite documenti di identità).

La corretta applicazione di un presidio privacy *compliant* potrà emergere dalla istituzione di un *team privacy* composto da: DPO, esperto informatico (responsabile ICT) capo responsabile aziendale della funzione *compliance* e responsabile del trattamento (che in molti casi corrisponde al Direttore HR). Il *team privacy* dovrà essere reperibile e operativo già nella fase di avvio di ispezione, ciò per evitare o, almeno, limitare i rischi di incorrere in contestazioni sanzionatorie.

Attenzione:

È consigliabile che il Titolare del trattamento individui la figura appartenete al *team privacy* cui affidare l'incarico preciso di fungere da interfaccia con le Autorità di controllo.

È auspicabile che tale incarico sia assegnato al DPO (ove nominato).

Oltretutto, la previsione di un "protocollo di attivazione" del *team privacy* aziendale è, di per sé, segnale di *compliance*. Gli ispettori, infatti, potranno constatare l'adozione di un protocollo di attivazione che,

evidentemente si applicherà anche in caso di *data breach*.

Attenzione:

Il consiglio è quello di chiedere di poter leggere e di verificare la correttezza delle dichiarazioni rilasciate e verbalizzate. Tanto più che la dicitura presente in calce al verbale *"letto e sottoscritto"* (anche dalla parte e dai presenti) lascerebbe scarso adito a ipotesi di incongruenza tra quanto dichiarato (dalla parte) e quanto scritto – *rectius*, verbalizzato – (dal Pubblico Ufficiale).

In ogni caso, è bene sapere che la parte ha a disposizione – in linea generale - **quindici giorni (a partire dalla data di apertura delle operazioni di ispezione) per produrre la documentazione** eventualmente richiesta dagli ispettori.

Attenzione:

Si consiglia di tenere in massima considerazione il rispetto di tale scadenza che – oltretutto – denota la corretta attuazione del principio di *accountability,* la incapacità – dichiarata, più o meno esplicitamente – di reperire i documenti richiesti sarebbe un evidente segnale di "non *compliant".*

Inoltre, si consiglia di consegnare solo copia della documentazione richiesta, in quanto l'originale dovrà essere – eventualmente – esibito in sede di ispezione.

b) Provvedimenti del Garante: sanzioni e provvedimenti correttivi

La **fase post-ispettiva** è quella in cui l'Autorità Garante per la protezione dei dati personali esercita il potere di comminare le sanzioni amministrative pecuniarie o di emanare i provvedimenti correttivi.

Rispetto all'applicazione delle **sanzioni pecuniarie**, l'art. 166 del Codice privacy ne attribuisce la **competenza al Garante per la privacy** che potrà, quindi, irrogare le sanzioni pecuniarie previste dall'art. 83 del GDPR e i provvedimenti correttivi di cui all'art. 58 paragrafo 2 del GDPR.
Lo stesso menzionato art. 166 Codice privacy sancisce che sono soggette alla sanzione amministrativa dell'art. 83 paragrafo 4 del GDPR, ovvero fino a 10 milioni di euro o per le imprese fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, le violazioni di cui agli articoli 2-*quinquies*, comma 2, 2-*quinquiesdecies*, 92, comma 1, 93, comma 1, 123, comma 4, 128, 129, comma 2, e 132-*ter*, nonché la mancata effettuazione della DPIA nei casi previsti dall'art. 110 comma primo.
Il paragrafo 5 dell'art. 83 GDPR prevede le sanzioni di maggiore entità, ovvero fino a 20 milioni di euro o per le imprese fino al 4% del fatturato, applicabili alle violazioni più gravi.

In fase di applicazione delle sanzioni pecuniarie, il Garante dovrà considerare, oltre alle circostanze del caso in esame, anche le caratteristiche del soggetto trasgressore e la collaborazione eventualmente

prestata, ancora, l'entità del danno arrecato agli interessati e il numero degli interessati esposti ai rischi della violazione.

in tal modo, il Garante potrà valutare l'ammontare della sanzione da comminare garantendo, così, che la sanzione sia *effettiva, proporzionata e dissuasiva,* così come previsto dal legislatore comunitario nel testo del Regolamento generale.

Attenzione: vi sono fattispecie suscettibili di poter essere verificate "da remoto" da parte dell'Autorità di controllo.

Si pensi, ad esempio, alla violazione di quanto previsto dal comma 7 dell'art. 37 del GDPR che pone l'obbligo per il titolare o responsabile del trattamento di rendere pubblici i dati di contatto del proprio *Data Protection Officer* (DPO) e di comunicarli all'Autorità Garante per la Protezione dei Dati Personali (la fattispecie si applica nei casi in cui la nomina del DPO sia obblifigatoria).

Tale violazione prevede una sanzione amministrativa fino a € 10.000.000 o al 2% del fatturato mondiale (ove superiore) per il trasgressore.

Per non incorrere in tale violazione:

2) i dati di contatto del DPO, possono essere resi pubblici mediante pubblicazione sul sito *web* istituzionale di un'apposita pagina dedicata all'esercizio dei diritti dell'interessato o tramite il loro inserimento nell'informativa privacy e la pubblicazione di quest'ultima *on-line*;
3) la comunicazione del nominativo del *Data Protection Officer* al Garante Privacy, deve essere effettuata mediante una procedura di invio telematico. Il Garante per la Privacy ha istituito un sistema di Comunicazione dei dati di contatto del Responsabile della Protezione dei Dati – RPD o DPO.

In virtù degli artt. 58.2 GDPR e 166.3 del Codice privacy, Garante può adottare una serie di provvedimenti correttivi. Si tratta del **potere di rivolgere avvertimenti al titolare o al responsabile** del trattamento sulla base di quei trattamenti considerati a rischio di violazione delle disposizioni del GDPR. In questi casi, il Garante può rivolgere ammonimenti o ingiungere di dare riscontro alle richieste avanzate dall'interessato, inn ordine – per esempio – all'esercizio dei diritti previsti dal GDPR.

Nel caso in cui l'Autorità di controllo dovesse ritenere configurati gli elementi da cui emergerebbe la violazione (o le violazioni) previste dal Codice Privacy o dall'art. 83 GDPR, ai sensi dell'art. 166 del Codice, dovrà procedere alla notifica al titolare o al responsabile del trattamento delle presunte violazioni *"salvo che la previa notifica non sia compatibile con la natura del provvedimento che intende adottare"*.

Attenzione:

Il titolare o responsabile del trattamento al quale sia stata notificata la presunta violazione, entro trenta giorni dal ricevimento, potrà inviare al Garante scritti difensivi o documenti e chiedere di essere ascoltato.

Al termine della fase istruttoria, dopo aver esaminato le dichiarazioni difensive della parte, il Garante potrà decidere di comunicare il provvedimento sanzionatorio (ordinanza-ingiunzione). In tal caso, il trasgressore dispone di trenta giorni per potersi adeguare alle prescrizioni del Garante ed effettuare il pagamento di un importo pari alla metà della sanzione irrogata.

In alternativa, sempre nel termine perentorio di trenta giorni, il trasgressore ha facoltà di proporre ricorso innanzi all'Autorità Giudiziaria, presso il Tribunale del luogo ove il titolare del trattamento risiede oppure del luogo di residenza dell'interessato.

Attenzione: il Garante può applicare la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione sul sito internet (ai sensi dell'art. 166 comma 7). Si tratta di una circostanza che rischierebbe di intaccare la reputazione dell'impresa o dello studio professionale destinatario della sanzione.

Il novellato Codice della privacy, inoltre, prevede alcune **violazioni che assumono rilevanza penale.**

- Trattamento illecito di dati
- Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala
- Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala
- Interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante
- Inosservanza di provvedimenti del Garante
- Violazioni in materia di controlli a distanza dei lavoratori e di indagine sulle loro opinioni
- False attestazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante
- Inosservanza di provvedimenti del Garante

Conclusioni e considerazioni del curatore editoriale

Il Regolamento UE n. 679/2016 (GDPR) sul trattamento e protezione dei dati personali, formalmente in vigore dal 24 maggio 2016 ed effettivamente applicabile dal 25 maggio 2018, ha – di fatto – ridisegnato i profili evolutivi della gestione dei dati personali e dell'attività di *data protection*. Il cuore pulsante di questo nuovo Regolamento – a parere di chi scrive – è rappresentato da quella "cultura della privacy" alla quale sistematicamente fa riferimento lo stesso Garante nazionale, Antonello Soro.

L'approccio al rinnovato impianto normativo per la corretta gestione dei dati personali deve fare leva sul "punto fermo" che è rappresentato proprio dalla **"Cultura della privacy".** Quanto più sviluppata e diffusa sarà la cultura della privacy, tanto più effettiva sarà la garanzia di protezione e di tutela dei dati personali delle persone fisiche.

La protezione dei dati, dunque, deve essere intesa – prima di tutto - come una necessità, la **necessità di tutela i diritti fondamentali dell'individuo**. Ma la protezione dei dati personali assume nella moderna società – definita "società dell'informazione" – un significato, oltre che sociale e giuridico, anche economico-competitivo e strategico.

Lo sanno bene quelle imprese e quei professionisti che considerano la capacità di proteggere i dati personali come un *asset* competitivo, capace di generare nei propri clienti/utenti/assistiti un sentimento di fiducia che è alla base dei rapporti professionali (si pensi al rapporto tra assistito e il suo avvocato – per l'appunto - di fiducia) e, persino, ai rapporti commerciali (si pensi, alle scelte di acquisto di prodotti o di abbonamento a servizi cui quotidianamente ci sottoponiamo come consumatori/clienti).

Con questo volume, gli Autori hanno voluto offrire un'analisi metodologica, concentrando la propria attenzione - e richiamando quella del lettore – verso un settore specifico di operatività del GDPR: l'ambiente di lavoro. Il lettore potrà facilmente accorgersi di come l'osservazione del quadro normativo di riferimento abbia – volutamente – dovuto risentire dell'effetto eclissi esercitato dall'approfondimento tecnico-operativo dedicato agli istituti che danno concreta attuazione al GDPR e al Codice privacy, in particolare, in ambiente lavorativo (studio professionale e azienda). Il risultato è un vero e proprio *vademecum* che potrà risultare di pronta utilità per il professionista, titolare di studio; per l'imprenditore, manager d'impresa; per i direttori del personale e i suoi stretti collaboratori, che potranno adeguare l'operatività delle proprie mansioni sulla base delle preziose indicazioni riportate in questo testo; nonché per i lavoratori dipendenti e per i collaboratori di studio che avranno modo di

conoscere appieno l'importanza di una efficace tutela dei propri dati personali, anche quando a gestirli e il loro datore di lavoro e di quali strumenti giuridici potranno avvalersi in caso di disallineamento tra le teoria e la pratica.

Giuseppe Miceli

Sitografia

- https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment
- https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf
- https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9080970
- https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento#6
- https://www.garanteprivacy.it/documents/10160/10704/Provvedimento+in+materia+di+videosorveglianza+-+leaflet+.pdf/6c3df7ec-7f25-4d5f-9ef9-eaebf6e9f0df?version=1.2
- https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1364939
- https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9124510
- https://www.garanteprivacy.it/home/ricerca/-/search/key/videosorveglianza
- https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3474069
- https://www.garanteprivacy.it/documents/10160/0/ALLEGATO+1+Elenco+delle+tipologie+di+trattamenti+soggetti+al+meccanismo+di+coerenza+da+sottoporre+a+valutazione+di+impatto.pdf/b9ceefa9-dd65-df86-fed4-df3c3570f59d?version=1.11
- https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4535524
- https://www.ispettorato.gov.it/it-it/orientamentiispettivi/Documents/Circolari/INL-Circolare-n-5-del-19-febbraio-2018-Videosorveglianza-signed.pdf

Formulario

(Scarica le formule in formato word)

Il reclamo

MODELLO DI RECLAMO*

AL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
P.ZZA VENEZIA, 11
00187 ROMA

Reclamo ex art. 77 del Regolamento (Ue) 2016/679 e artt. da 140-bis a 143 del Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento

Il/La sottoscritto/a....., nato/a a .....il ....., residente in..... CF....., il/la quale ai fini del presente procedimento dichiara di voler ricevere eventuali comunicazioni al seguente recapito (indicare uno o più recapiti, tra indirizzo fisico, telefono, e-mail, fax) espone quanto segue:

(in questa parte del reclamo dovranno essere forniti necessariamente i seguenti elementi:)

a) dichiarazione in relazione alla circostanza che la Repubblica italiana è lo Stato membro in cui risiede abitualmente, lavora oppure il luogo ove si è verificata la presunta violazione;

b) gli estremi identificativi del titolare del trattamento (cioè, 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 e che avrebbe commesso la violazione);

c) gli estremi identificativi del responsabile del trattamento (ove conosciuto);

d) un'indicazione, per quanto possibile dettagliata, dei fatti e delle circostanze su cui l'atto si fonda, ivi comprese eventuali richieste già rivolte sulla questione al Titolare del trattamento;

e) le disposizioni del Regolamento (Ue) 2016/679 e del Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento che

si presumono violate, specificando se siano stati già eventualmente esercitati i diritti di cui agli artt. da 15 a 22 del Regolamento, e l'indicazione delle misure richieste.

Tutto ciò premesso, il/la sottoscritto/a:

CHIEDE

al Garante per la protezione dei dati personali, esaminato il reclamo che precede e ritenutane la fondatezza, di assumere nei confronti di …….(indicare il titolare del trattamento, recapito, ed ogni elemento utile alla sua individuazione) ogni opportuno provvedimento e, in particolare:

a) rivolgere a questi o al responsabile del trattamento avvertimenti o ammonimenti sul fatto che detti trattamenti possono verosimilmente violare, ovvero abbiano violato, le disposizioni vigenti in materia;

b) ingiungere al titolare del trattamento di soddisfare le richieste di esercizio dei diritti di cui agli artt. da 15 a 22 del Regolamento e/o di conformare i trattamenti alle disposizioni vigenti in materia anche nei confronti del responsabile del trattamento, ove previsto;

c) imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento.

Elenco dei documenti allegati:

1)

2)

3)

Data

Firma

* Il reclamante potrà far pervenire l'atto utilizzando la modalità ritenuta più opportuna, consegnandolo a mano presso gli uffici del Garante (all'indirizzo di seguito indicato) o mediante l'inoltro di: a) raccomandata A/R indirizzata a: Garante per la protezione dei dati personali, Piazza Venezia, 11 - 00187 Roma b) messaggio di posta elettronica certificata indirizzata a: protocollo@pec.gpdp.it

Incarico al responsabile esterno

NOMINA RESPONSABILE ESTERNO DEL TRATTAMENTO

ai sensi dell'art. 28 del Regolamento Europeo 2016/679 (in seguito anche "GDPR")

tra

La Società XY (P. IVA-C.F. _____; tel. _____; fax _____; mail _____), con sede in _____, Titolare del trattamento ai sensi dell'art. 4 comma 1 n. 7 GDPR, in persona del legale rappresentante _____

e

_____ (C.F. _____ - P.I. _____), con sede in _____, in persona del legale rappresentante _____, Responsabile del trattamento ai sensi dell'art. 28 GDPR

[*Oppure, in caso di persona fisica*]

_____ (C.F. _____ - P.I. _____), con sede in _____, Responsabile del trattamento ai sensi dell'art. 28 GDPR

premesso che

- in forza del contratto/incarico stipulato in data _____ (di seguito denominato il "Contratto"), il Titolare del trattamento si avvale di _____, per i servizi di _____ (di seguito, i "Servizi");
- l'espletamento dei Servizi comporta un trattamento di dati personali, come definiti all'art. 4 comma 1 GDPR, che _____ deve svolgere per conto del Titolare;
- il GDPR e il Codice privacy impongono una serie di obblighi e vincoli al trattamento di dati personali da parte del Titolare che anche il Responsabile è tenuto a rispettare;
- che _____ ha dimostrato di offrire garanzie sufficienti in ordine all'adozione di misure tecniche e organizzative adeguate per far sì che il trattamento dei dati sia conforme alle disposizioni del GDPR e sia idoneo alla tutela dei diritti dell'interessato;
- che con il presente atto di nomina (di seguito l'"Atto") il Titolare del trattamento intende dunque procedere alla nomina di _____ quale Responsabile del trattamento, impartendogli dettagliate istruzioni in relazione al trattamento dei dati.

Tutto ciò premesso si
conviene quanto segue

1. Nomina a Responsabile del trattamento

Con il presente Atto il Titolare del trattamento _____ nomina, ai sensi dell'art. 28 GDPR, _____ quale Responsabile del trattamento dei dati, in relazione ai tutti i trattamenti di dati che sono necessari allo svolgimento dei Servizi di cui al Contratto.

2. Caratteristiche del trattamento

Il trattamento è consentito per tutto il tempo necessario all'esecuzione dei Servizi oggetto del Contratto ed è necessario in particolare al perseguimento delle seguenti finalità:

a) _____;
b) _____.

Il trattamento potrà avere a oggetto dati personali comuni e, ove necessario, dati personali "particolari", e potrà essere svolto in via cartaceo o informatica.

3. Obblighi del Responsabile del trattamento

Il Responsabile del trattamento è tenuto, ai sensi dell'art. 28 terzo comma GDPR, a:

a) trattare i dati personali trasmessi dal Titolare o comunque acquisiti in relazione al Servizio da svolgere in corrispondenza alle istruzioni del Titolare e agli obblighi previsti dal presente Atto, informando comunque immediatamente il Titolare qualora, a suo parere, un'istruzione impartita violi il GDPR o la normativa italiana sulla protezione dei dati;
b) individuare e nominare per iscritto le persone autorizzate al trattamento all'interno della propria struttura ("Sub-responsabili") e garantire che i predetti Sub-responsabili si impegnino alla riservatezza dei dati o abbiano un adeguato obbligo legale di riservatezza e si impegnino altresì all'adozione delle misure di sicurezza adottate e al rispetto dei principi del trattamento dei dati di cui al Capo II del GDPR;
c) adottare e descrivere al Titolare tutte le misure di sicurezza richieste dall'art. 32 GDPR, ritenute idonee al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
d) informare il Titolare della nomina di propri Responsabili al trattamento ("sub-Responsabili") nonché della loro successiva sostituzione con nuovi Responsabili, al fine di permettere al Titolare di valutare l'idoneità degli stessi ed eventualmente opporsi alla nomina o sostituzione. In caso di nomina autorizzata di altro Responsabile, a individuare le specifiche attività di trattamento del Responsabile e a stipulare con il Responsabile apposito contratto con il quale il Responsabile assuma, in relazione ai trattamenti svolti, gli stessi obblighi previsti nel presente Accordo;
e) collaborare con il Titolare, con misure tecniche e organizzative adeguate, ove possibile, al fine di soddisfare l'obbligo del Titolare di dare seguito alle richieste per l'esercizio dei diritti dell'interessato descritti negli artt. da 15 a 22 GDPR, con le modalità di cui all'art. 12 GDPR e le tempistiche indicate nell'art. 12 terzo comma GDPR. A tal fine, il Responsabile trasmette le eventuali richieste degli interessati, all'indirizzo mail del Titolare _____ entro 24 ore dal ricevimento della richiesta;
f) in relazione al trattamento svolto, assistere e collaborare con il Titolare ai fini del rispetto degli obblighi imposti al Titolare dagli artt. da 33 a 36 GDPR, ed in particolare:
   - informare il Titolare, senza ingiustificato ritardo, e comunque al più tardi entro 24 ore dal momento in cui ne è venuto a conoscenza, all'indirizzo mail del Titolare _____ di ogni violazione di dati personali, al fine di permettere al Titolare la notifica al Garante per la Protezione dei Dati Personali ai sensi dell'art. 33 GDPR e, se del caso, la comunicazione all'interessato ai sensi dell'art. 43 GDPR, fornendo tutte le informazioni sulla predetta violazione che siano a sua conoscenza tra quelle indicate dall'art. 33 comma 3 GDPR;
   - assistere e collaborare con il Titolare nel processo di eventuale valutazione d'impatto sulla protezione dei dati ("DPIA – *Data Protection Impact Assessment*") di cui all'art. 35 GDPR, nonché nella eventuale fase di consultazione preventiva con l'Autorità di controllo ai sensi dell'art. 36 GDPR, qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare per attenuare il rischio;
g) cancellare o restituire tutti i dati personali una volta cessata in via definitiva l'esecuzione dei Servizi e cancellare le copie esistenti secondo le istruzioni ricevute dal Titolare, salvo che la conservazione dei dati sia prevista dal diritto UE o dalla normativa italiana;
h) mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto, da parte del Responsabile, degli obblighi di cui al presente Atto e contribuire alle attività di revisione, comprese le ispezioni, poste in essere dal Titolare.

Il Responsabile del trattamento è tenuto, ove sussistano le condizioni di cui all'art. 30 comma 5 GDPR, alla redazione e al costante aggiornamento di un "Registro delle attività di trattamento" svolte per conto del Titolare, in forma scritta, anche in formato elettronico, da tenere a disposizione in ogni momento del Titolare, con il contenuto di cui all'art. 30, comma 2, GDPR.

Il Responsabile del trattamento è altresì tenuto:

- ove compia una autonoma valutazione d'impatto sulla protezione dei dati ("DPIA *Data Protection Impact Assessment*") di cui all'art. 35 GDPR in relazione ai propri servizi, prodotti, asset che coinvolgano

i trattamenti compiuti per conto del Titolare, a comunicare tempestivamente al Titolare il report finale della DPIA svolta;
- a informare tempestivamente il Titolare qualora intenda avvalersi di servizi "*Cloud*" per il trattamento dei dati personali, assicurandosi altresì che i dati stessi vengano conservati all'interno dell'UE.

Il Responsabile si impegna altresì a valutare, ai fini della dimostrazione della propria idoneità all'incarico, l'adesione ad eventuali codici di condotta o ad un meccanismo di certificazione approvati ai sensi dell'art. 40 e 42 GDPR.

4. Principi del trattamento dei dati

Il Responsabile del trattamento è tenuto, in relazione a tutti i trattamenti svolti per conto del Titolare, al rispetto dei principi di cui al Capo II del GDPR, nonché a consentire al Titolare di poter dimostrarne il rispetto nei confronti degli interessati e del Garante per la Protezione dei dati personali.

A titolo esemplificativo e non esaustivo si precisa che i dati:
- devono essere trattati in modo lecito, corretto e trasparente;
- devono essere raccolti solo per le finalità del trattamento, svolto dal Responsabile, che siano determinate, esplicite e legittime;
- devono essere adeguati, pertinenti e non eccedenti rispetto alle finalità;
- devono essere esatti e se necessario aggiornati;
- devono essere conservati per un periodo non superiore a quello necessario al raggiungimento delle finalità del trattamento. Trascorso detto periodo i dati vanno resi anonimi o cancellati;
- se comuni vanno trattati nei casi indicati all'art. 6 GDPR;
- se "particolari" vanno trattati nei casi indicati dall'art. 9 e 10 GDPR.

Il Responsabile è altresì tenuto al rispetto degli obblighi di informativa all'interessato ai sensi dell'art. 13 comma 2 GDPR e di acquisizione del consenso nei casi previsti dall'art. 7, 8, 9 e 10 GDPR, nonché a garantire all'interessato, in relazione ai trattamenti svolti per conto del Titolare, l'esercizio dei diritti previsti dagli artt. 15, 16, 17, 18, 20, 21 GDPR.

Il Responsabile è comunque tenuto e ha il potere di svolgere ogni incombenza connessa all'esecuzione dell'incarico di cui al presente Accordo che sia necessaria o opportuna per l'esercizio dei compiti indicati nel presente Accordo.

5. Disposizioni generali e finali

Le Parti dichiarano di aver letto e pienamente compreso il contenuto del presente Atto e di esprimere pienamente, con la sottoscrizione, il loro consenso. Eventuali modifiche al presente Atto, se del caso anche mediante l'inserimento di "clausole tipo" di cui all'art. 28 comma 6 GDPR, dovranno essere apportate esclusivamente per iscritto.

L'invalidità, anche parziale, di una o più delle clausole del presente Atto non pregiudica la validità delle restanti clausole.

L'incarico di Responsabile del trattamento dei dati è di carattere fiduciario e non è quindi suscettibile di delega, salva la nomina di sub-responsabili ai sensi del presente Atto. L'incarico di Responsabile del Trattamento cessa automaticamente alla scadenza o alla cessazione del Contratto e/o del Servizi affidati, salvi gli obblighi attinenti al trattamento dei dati da considerarsi esistenti anche successivamente alla cessazione del rapporto.

Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni in materia di protezione dei dati personali di cui al GDPR e al D.Lgs. n. 196 del 29.7.2003 (Codice in materia di protezione dei dati personali).

Per accettazione dell'incarico
Il Responsabile del trattamento

_____

Il Titolare del trattamento
Società XY (timbro)
Il Legale Rappresentante

_____

Informativa ai dipendenti

Egr. Signore/a,
ai sensi dell'art. 13 del Regolamento UE 2016/679 in materia di protezione dei dati personali ("GDPR") La informiamo di quanto segue.

A) **Finalità del trattamento e base giuridica**. La Società XY tratterà i dati personali che La riguardano o da Lei conferiti esclusivamente nell'ambito del rapporto di lavoro o della collaborazione professionale (ai fini dell'adempimento degli obblighi contrattuali e di legge, per la corrispondenza e per la rintracciabilità, per l'organizzazione del servizio, ecc.). La base giuridica è rappresentata dal contratto di lavoro (art. 6, comma 1, lett. b e art. 9 comma 2 lett. b GDPR), dagli obblighi legali a cui è tenuta la Società XY (art. 6 comma 1 lett. c GDPR) e dal consenso (art. 6 comma 1 lett. a e art. 9 comma 2 lett. a GDPR).

B) **Dati particolari**. Il trattamento di Suoi eventuali dati "particolari" e relativi alla salute sarà effettuato nei limiti di cui all'art. 9 comma 2 lett. b) e lett. h GDPR e quindi solo ove il trattamento sia necessario per assolvere gli obblighi ed esercitare i diritti in materia di diritto del lavoro, sicurezza sociale e protezione sociale.

A) **Modalità e principi del trattamento**. Il trattamento avverrà nel rispetto del GDPR e del D.Lgs. n. 196/03 ("Codice in materia di protezione dei dati personali"), nonché dei principi di liceità, correttezza e trasparenza, adeguatezza e pertinenza, con modalità cartacee e informatiche, ad opera di persone autorizzate dalla La Società XY e con l'adozione di misure adeguate di protezione, per garantire la sicurezza e la riservatezza dei dati. [EVENTUALMENTE FAR PRESENTE CHE: Non verrà svolto alcun processo decisionale automatizzato].

C) **Necessità del conferimento. Comunicazione e trasferimento all'estero dei dati.** Il conferimento dei dati è necessario in quanto strettamente legato all'organizzazione del servizio e alla gestione del rapporto di lavoro. *La pubblicazione del cognome e nome, del ruolo e dell'indirizzo e-mail sul sito della Società XY, nei social network (es. pagina Facebook/Instagram/Youtube) e sul materiale informativo cartaceo della Società XY è invece facoltativa e avviene solo previo esplicito e specifico consenso*. I dati potranno essere comunicati a tutti i soggetti deputati allo svolgimento di attività a cui la Società XY è tenuta in base ad obbligo di legge (commercialista, consulente del lavoro, assicuratore, sistemista, ecc.) e a tutte quelle persone fisiche e/o giuridiche, pubbliche e/o private quando la comunicazione risulti necessaria o funzionale allo svolgimento dell'attività istituzionale e alla gestione del rapporto di lavoro (I.N.P.S., I.N.A.I.L., formatori, Enti Locali, Enti sanitari, fornitori, ecc.). Ove necessario o opportuno, i soggetti cui vengono trasmessi i dati per lo svolgimento di attività per conto della Società XY saranno nominati Responsabili (esterni) del trattamento ai sensi dell'art. 28 GDPR. I dati potranno essere trasferiti a destinatari con sede extra UE che hanno sottoscritto accordi diretti ad assicurare un livello di protezione adeguato dei dati personali, o comunque previa verifica che il destinatario garantisca adeguate misure di protezione.

D) **Periodo di conservazione dei dati**. I dati saranno utilizzati dalla Società XY per tutta la durata del rapporto lavorativo. Dopo tale data, saranno conservati i soli dati la cui conservazione risponde a obblighi legali o contabili o fiscali o a esigenze di tutela della Società XY.

E) **Diritti dell'interessato**. Nella qualità di Soggetto interessato, Le sono garantiti tutti i diritti specificati all'art. 15 - 20 GDPR [E' NECESSARIO RIPORTATER IL TESTO DEI PREDETTI ARTICOLI DEL GDPR, SI CONSIGLIA DI ATTIVARE UN COLLEGAMENTO IPEERTESTUALE], tra cui il diritto all'accesso, rettifica e cancellazione dei dati, il diritto di limitazione e opposizione al trattamento, il diritto di revocare il consenso al trattamento (senza pregiudizio per la liceità del trattamento basata sul consenso acquisito prima della revoca), nonché il di proporre reclamo al Garante per la Protezione dei dati personali qualora tu ritenga che il trattamento che ti riguarda violi il GDPR o la normativa italiana. I suddetti diritti possono essere esercitati mediante comunicazione scritta [SI CONSIGLIA DI ATTIVARE UN COLLEGAMENTO IPEERTESTUALE CHE RIMANDI L'INTERESSATO AL MODULO EDITABILE] da inviare a mezzo *posta elettronica, p.e.c. o fax*, o a mezzo Raccomandata presso la sede della Società XY.

F) *Il **Data Protection Officer** (DPO)* nominato dalla Società XY è _____, a cui ciascun interessato può scrivere, in relazione al trattamento dei dati svolto dalla Società XY e/o in relazione ai Suoi diritti, all'indirizzo _____. Il DPO può essere altresì contattato telefonicamente tramite l'Associazione al numero _____.

G) **Titolare del trattamento**. Il titolare del trattamento è la Società XY _____, con sede in _____ – tel. _____ – fax _____ – mail _____

CONSENSO AL TRATTAMENTO DEI DATI PERSONALI

Io sottoscritto/a, _____, nella qualità di interessato, letta la suddetta informativa resa ai sensi dell'art. 13 GDPR, **autorizzo e presto consenso**

□ al trattamento dei miei dati personali, da svolgersi in conformità a quanto indicato nella suddetta informativa e nel rispetto delle disposizioni del GDPR e del D.Lgs. n. 196/03 **(*)**

□ *alla diffusione del mio nome e cognome, ruolo e immagine fotografica sul sito istituzionale della Società XY* **(**)**

□ *alla diffusione della mia immagine o di video che mi riprendono nel sito istituzionale, nei social network (es. pagina Facebook/Instagram/Youtube) e sul materiale informativo cartaceo della Società XY, per soli fini di descrizione e promozione dell'attività istituzionale, nel rispetto delle disposizioni del GDPR e del D.Lgs. n. 196/03 e delle autorizzazioni/indicazioni della Commissione UE e del Garante per la Protezione dei Dati Personali* **(**)**

_____, lì _____

L'INTERESSATO
(firma leggibile)

_____

(*) Il consenso al trattamento è indispensabile ai fini della gestione del rapporto di lavoro
(**) Il consenso al trattamento è facoltativo
N.B. Le parentesi quadre contengono avvertenze e consigli per la corretta compilazione del documento.

Segnale video sorveglianza informativa

Esempio:

Identità del Titolare del trattamento:

Dettagli di contatto del Data Protection Officer (DPO/RPD) ove applicabile:

Finalità del trattamento dati personali nonché fonti normative per l'elaborazione:

Diritti dell'interessato: *Sono i diversi diritti dell'interessato al trattamento nei confronti del Titolare, in particolare il diritto di accesso o cancellazione dei dati personali.*

Per tutti i dettagli su questo servizio di videosorveglianza, inclusi i tuoi diritti, consulta le informazioni complete fornite dal Titolare attraverso le opzioni riportate a sinistra.