ORDINE INGEGNERI BOLOGNA

in collaborazione con

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI ANCONA

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI FERRARA

Ordine degli Ingegneri della provincia di Forlì Cesena

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI RAVENNA

ORDINE INGEGNERI REGGIO EMILIA

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI RIMINI

presenta

TRATTAMENTO DEI DATI PERSONALI IN CONFORMITÀ CON IL REGOLAMENTO EUROPEO 2016/679 (GDPR)

LINEE GUIDA PER I PROFESSIONISTI

VERSIONE 1.0 DEL 10/10/2018

Comitato di redazione

Coordinamento

- **Ing. Francesca Merighi**, *Coordinatrice area tematica sicurezza delle informazioni e protezione dei dati personali, Ordine degli Ingegneri di Bologna*

Membri

- **Ing. iunior Michele Bruno**, *membro delle commissioni di Federazione Regionale Ordini Ingegneri dell'Emilia Romagna: industria - industria 4.0, informazione e, qualità - management - certificazione; consigliere del Consiglio di Disciplina dell'Ordine degli Ingegneri della Provincia di Rimini*
- **Dott.ssa Claudia Cevenini**, *Professoressa a contratto di Diritto dell'informatica, Dipartimento di Informatica - Scienza e Ingegneria - DISI dell'Università di Bologna*
- **Ing. Fabrizio Di Crosta**, *membro dell' area tematica sicurezza delle informazioni e protezione dei dati personali e Data Protection Officer dell'Ordine degli Ingegneri di Bologna*
- **Ing. Rita Amelia Grunspan**, *consigliere dell'Ordine degli Ingegneri di Ancona*
- **Avv. Laura Lecchi**, *Cultore della Materia di Diritto dell'informatica, Scuola di Ingegneria dell' Università di Bologna*
- **Ing. Matteo Pedretti**, *consigliere dell'Ordine degli Ingegneri di Reggio Emilia*
- **Ing. Massimo Piceni**, *consigliere dell'Ordine degli Ingegneri di Forlì-Cesena*
- **Ing. Massimiliano Rossi**, *consigliere dell'Ordine degli Ingegneri di Reggio Emilia*
- **Ing. Rosario Russo**, *membro e Data Protection Officer dell'Ordine degli Ingegneri di Ferrara*
- **Ing. Mattia Sangiorgi**, *consigliere dell'Ordine degli Ingegneri di Ravenna*
- **Ing. Marco Schonhaut**, *membro dell'area tematica sicurezza delle informazioni e protezione dei dati personali, Ordine degli Ingegneri di Bologna*

Autori e contributori

- **Ing. Francesca Merighi**
- **Ing. iunior Michele Bruno**
- **Dott.ssa Claudia Cevenini**
- **Ing. Fabrizio Di Crosta**
- **Ing. Rita Amelia Grunspan**
- **Avv. Laura Lecchi**
- **Ing. Massimo Piceni**
- **Ing. Marco Schonhaut**

Proprietà intellettuale

Indice degli argomenti

1. CONTESTO

Le linee guida che seguono sono state pensate e predisposte per essere **destinate ai liberi professionisti o titolari di studi professionali che operano in settori esclusi quelli sanitari**, allo scopo di supportarli negli adempimenti derivanti dal trattamento dei dati personali nell'esercizio della propria attività lavorativa, in conformità con la normativa applicabile.

Esse riportano estratti della normativa vigente e di documentazione ad essa correlata. **I testi riportati sono stati rielaborati** (contengono riferimenti, note del redattore e omissis) al fine di garantire una più facile lettura e comprensione da parte del lettore.

L**e linee guida** si prefiggono l'intento ambizioso di orientare ed indicare le traiettorie da seguire nell'adeguamento alle norme europee e nazionali in materia. Considerato che le scienze giuridiche non possono considerarsi esatte, perché mutevoli nel tempo e nello spazio e nella interpretazione, a tutt'oggi ancora indefinita, agli Ordini professionali, agli autori, ai revisori e a tutti coloro che hanno partecipato con i propri contributi, alla costruzione delle Linee guida dal contenuto e dal valore orientativo, dunque di mero supporto nell'applicazione delle norme in materia di privacy, che dunque **non può costituire, nè sostituire** un parere od una consulenza legale, né la **consulenza di esperti in ambito di protezione del trattamento dei dati personali, privacy e diritto delle nuove tecnologie informatiche**. Pertanto non essendo altro che linee guida a supporto, l'uso, l'osservanza o la consultazione delle stesse non potrà garantire la conformità all'adempimento esatto delle norme, in ordine alla quale alcuna responsabilità giuridica potrà essere ascritta agli autori, manlevati, anche con esclusione del diritto di rivalsa, per eventuali divergenze interpretative o l'applicazione inadeguata e difforme dei suggerimenti che recano.

Alla stessa stregua gli Autori, gli Ordini e i Revisori, garantiscono la paternità dei propri contributi, che come tali soggiacciono alle tutele delle norme in materia di diritto d'autore.

2. DOCUMENTAZIONE DI RIFERIMENTO

2.1. Normativa europea

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) di seguito richiamato con il termine ***Regolamento***.

2.2. Normativa italiana

DECRETO LEGISLATIVO 10 agosto 2018, n. 101, recante "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, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)" (in G.U. 4 settembre 2018 n.205) di seguito richiamato con il termine ***Decreto 101/2018.***

DECRETO LEGISLATIVO 30 giugno 2003, n.196 recante il "Codice in materia di protezione dei dati personali" (in S.O n. 123 alla G.U. 29 luglio 2003, n. 174), aggiornato dal Decreto 101/2018***,*** di seguito richiamato con il termine ***Codice privacy.***

2.3. Provvedimenti generali del Garante

Il *Garante per la protezione dei dati personali* o comunemente *Garante della Privacy*, in seguito richiamato con il termine ***Garante***, è l'autorità di controllo nazionale italiana in materia di protezione dei dati personali.

ha emanato nel corso del tempo numerosi provvedimenti generali e linee guida intesi a integrare il disposto Codice Privacy e fornire un supporto per la sua corretta interpretazione e applicazione concreta.

A seguito dell'applicazione del Regolamento, e in seguito all'aggiornamento normativo a livello nazionale, tali documenti restano operativi, per quanto non in contrasto con il Regolamento e con l'evoluzione del quadro normativo italiano generale.

Si riporta di seguito una sintesi in ordine alfabetico dei principali documenti emanati dal Garante che possono essere di interesse per gli ingegneri sotto vari profili, es. in qualità di soggetti Titolari o Responsabili del trattamento, Responsabili della protezione dei dati incaricati, oppure nel loro ruolo di creatori o utilizzatori di tecnologie che implicano trattamento di dati personali.

E' indispensabile tenersi costantemente aggiornati e consultare frequentemente il sito web del Garante o iscriversi alla newsletter, per venire tempestivamente a conoscenza di tutti i futuri documenti che saranno emanati.

Conoscere il Regolamento e la normativa italiana di recente emanazione potrebbe non essere sufficiente per mettersi a norma: quanto disposto nei documenti emanati dal Garante costituisce un riferimento essenziale che deve essere preso in debita considerazione, ma soprattutto un fondamentale ausilio.

Amministratori di sistema

- Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 (aggiornato in base al provvedimento del 25 giugno 2009)

Banche

- Linee guida per trattamenti dati relativi al rapporto banca-clientela - 25 ottobre 2007

Biometria

- Provvedimento generale prescrittivo in tema di biometria - 12 novembre 2014

Cloud computing

- Cloud Computing - La guida del Garante della Privacy per imprese e pubblica amministrazione - 2012

Dati giudiziari

- Linee guida in materia di trattamento di dati personali nella riproduzione di provvedimenti giurisdizionali per finalità di informazione giuridica - 2 dicembre 2010
- Pubblicazione di intercettazioni telefoniche e dignità della persona - 21 giugno 2006
- Misure di sicurezza obbligatorie per le intercettazioni - 15 dicembre 2005

Dati sensibili

- Linee guida in materia di Dossier sanitario - 4 giugno 2015
- Linee guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione nei siti web esclusivamente dedicati alla salute - 25 gennaio 2012
- Linee guida in tema di trattamento di dati per lo svolgimento di indagini di customer satisfaction in ambito sanitario - 5 maggio 2011
- Linee guida in tema di referti on-line - 19 novembre 2009
- Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario - 16 luglio 2009
- Trattamento dei dati sensibili nella pubblica amministrazione - 30 giugno 2005
- Dati sanitari. Provvedimento generale sui diritti di 'pari rango' - 9 luglio 2003

Dati telefonici e telematici

- Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. data breach) – 4 aprile 2013
- Recepimento normativo in tema di dati di traffico telefonico e telematico - 24 luglio 2008
- Sicurezza dei dati di traffico telefonico e telematico - 17 gennaio 2008

Imprese

- Provvedimento in ordine all'applicabilità alle persone giuridiche del Codice in materia di protezione dei dati personali a seguito delle modifiche apportate dal d.l. n. 201/2011 - 20 settembre 2012
- Guida pratica e misure di semplificazione per le piccole e medie imprese - 24 maggio 2007

Informazioni commerciali

- Diritto di accesso - Prescrizioni di carattere generale per le 'centrali rischi private' - 31 luglio 2002

Internet e social media

- E-state in privacy - Informazioni utili su selfie e foto, protezione di smartphone e tablet, acquisti on line, uso di app, chat e social network quando si è in vacanza - 2018
- Cookie e privacy: istruzioni per l'uso - 2014-2015
- Chiarimenti in merito all'attuazione della normativa in materia di cookie - 5 giugno 2015
- Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie - 8 maggio 2014

Lavoro

- Lavoro: le linee guida del Garante per posta elettronica e internet - 10 marzo 2007
- Sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro - 4 ottobre 2011
- Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico - 14 giugno 2007
- Linee-guida per il trattamento di dati dei dipendenti privati - 23 novembre 2006
- Lavoro e previdenza sociale - Cartellini identificativi dei lavoratori - 11 dicembre 2000

Marketing

- Provvedimento generale a carattere prescrittivo sulle c.d. 'chiamate mute - 20 febbraio 2014
- Provvedimento prescrittivo in materia di trattamento dei dati personali effettuato mediante l'utilizzo di call center siti in Paesi al di fuori della Unione europea - 10 ottobre 2013
- Consenso al trattamento dei dati personali per finalità di "marketing diretto" attraverso strumenti tradizionali e automatizzati di contatto - 15 maggio 2013
- Prescrizioni per il trattamento di dati personali per finalità di marketing, mediante l'impiego del telefono con operatore, a seguito dell'istituzione del registro pubblico delle opposizioni - 19 gennaio 2011
- Titolarità del trattamento di dati personali in capo ai soggetti che si avvalgono di agenti per attività promozionali - 15 giugno 2011
- Trattamento dei dati degli abbonati in caso di number portability - 1° aprile 2010
- Adempimenti semplificati per il customer care Adempimenti semplificati per il customer care (inbound) - 15 novembre 2007
- Servizi telefonici non richiesti - 16 febbraio 2006
- 'Fidelity card' e garanzie per i consumatori. Le regole del Garante per i programmi di fidelizzazione - 24 febbraio 2005
- TV interattiva: misure necessarie ed opportune per un trattamento dei dati conforme alle disposizioni vigenti - 3 febbraio 2005
- Elenchi telefonici: garanzie e modalità per il trattamento dei dati personali -15 luglio 2004

- Linee guida in materia di attività promozionale e contrasto allo spam - 4 luglio 2013
- Spamming. Regole per un corretto uso dei sistemi automatizzati e l'invio di comunicazioni elettroniche - 29 maggio 2003

Misure di sicurezza

- Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali - 13 ottobre 2008

Profilazione

- Linee guida in materia di trattamento di dati personali per profilazione on line - 19 marzo 2015
- Aggiornamento delle prescrizioni dirette ai fornitori di servizi di comunicazione elettronica accessibili al pubblico che svolgono attività di profilazione - 6 febbraio 2014
- Prescrizioni ai fornitori di servizi di comunicazione elettronica accessibili al pubblico che svolgono attività di profilazione – 25 giugno 2009

Pubblica Amministrazione

- Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche - 2 luglio 2015
- Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati - 28 maggio 2014
- Linee guida per il trattamento di dati personali effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web - 2 marzo 2011
- Linee guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione di atti e documenti di enti locali - 19 aprile 2007

RFID

- Etichette intelligenti" (Rfid): il Garante individua le garanzie per il loro uso - 9 marzo 2005

Videosorveglianza

- Provvedimento in materia di videosorveglianza - 8 aprile 2010
- Videosorveglianza - Provvedimento generale - 29 aprile 2004
- Videosorveglianza - Il decalogo delle regole per non violare la privacy - 29 novembre 2000

2.4. Linee guida e documenti

2.4.1. Linee guida e documenti del Comitato europeo per la protezione dei dati

Il *Comitato europeo per la protezione dei dati* (ex Gruppo di lavoro Art. 29), di seguito richiamato con il termine **Comitato**, è un'istituzione indipendente, che contribuisce all'applicazione coerente

delle norme sulla protezione dei dati in tutta l'Unione europea e promuove la cooperazione tra le autorità competenti per la protezione dei dati dell'UE.

È composto da rappresentanti delle autorità nazionali per la protezione dei dati e dal *Garante europeo della protezione dei dati* (GEPD).

Il Comitato può adottare **orientamenti generali** per chiarire quanto disposto dalla normativa europea sulla protezione dei dati, fornendo un'interpretazione uniforme di diritti e obblighi dei destinatari.

Può anche adottare **decisioni vincolanti** ai sensi del Regolamento UE sulla privacy nei confronti delle Autorità nazionali di controllo (ad esempio il Garante) per garantire un'applicazione coerente delle norme.

Il Comitato - e precedentemente il Gruppo Art. 29 - pubblica Linee Guida e altri documenti che costituiscono un indispensabile supporto alla corretta interpretazione e applicazione della disciplina in materia di protezione dei dati personali, oltre a fornire indicazioni ed esempi di buone e cattive prassi.

Si riportano di seguito i principali documenti attualmente disponibili del Comitato e dell'Art. 29, come ratificati dal Comitato stesso. I documenti più recenti sono disponibili solo in lingua inglese.

2.4.1.1. Linee guida del Comitato europeo per la protezione dei dati

- Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 - 25 maggio 2018
  Fornisce indicazioni sull'applicazione dell'Articolo 49 del Regolamento in merito alle deroghe nel contesto dei trasferimenti di dati personali a paesi terzi.
- Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679 - 25 maggio 2018
  Non si tratta di un manuale procedurale per la certificazione in conformità con il Regolamento. Lo scopo principale di queste linee guida è identificare i criteri generali che possono essere rilevanti per tutti i meccanismi di certificazione emessi in conformità con gli artt. 42 e 43 del Regolamento.

2.4.1.2. Linee guida Gruppo Art. 29

Autorità garanti

- Guidelines on the Lead Supervisory Authority

Consenso

- Linee guida sul consenso ai sensi del regolamento (UE) 2016/679 (disponibili in italiano nel file .zip) - 10 aprile 2018
  Forniscono un'analisi approfondita della nozione di consenso. Il Regolamento fornisce ulteriori chiarimenti e specifiche sui requisiti per ottenere e dimostrare un consenso valido. Le linee guida forniscono orientamenti pratici per garantire il rispetto del Regolamento.

Decisioni individuali automatizzate

- Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679

DPO (Responsabile per la protezione dei dati)

- Guidelines on Data Protection Officers ('DPOs') - 5 aprile 2017
  Forniscono chiarimenti su quanto disposto dal Regolamento sia per aiutare i titolari e i responsabili del trattamento a conformarsi alla normativa vigente, sia per assistere i DPO nel loro ruolo. Forniscono anche raccomandazioni sulle migliori pratiche, basandosi sull'esperienza acquisita in alcuni Stati membri dell'UE. Il Comitato controllerà l'attuazione di queste linee guida e potrà integrarle con ulteriori dettagli, a seconda dei casi.

Portabilità dei dati

- Linee guida sul diritto alla portabilità dei dati (disponibili in italiano nel file .zip) - 5 aprile 2017
  Supportano i titolari nell'adempimento dei loro obblighi, forniscono raccomandazioni relative a migliori prassi e agli strumenti che possono essere d'ausilio nell'osservanza del diritto alla portabilità dei dati. Raccomandano inoltre alle imprese e alle associazioni di settore di collaborare per definire un insieme condiviso di standard e formati interoperabili che soddisfino i requisiti del diritto alla portabilità dei dati.

Sanzioni

- Guidelines on the application and setting of administrative fines (wp253)

Trasparenza (obblighi di informativa)

- Guidelines on Transparency under Regulation 2016/679 - 11 aprile 2018

Valutazione d'impatto

- Guidelines on Data Protection Impact Assessment (DPIA)

Violazione dei dati

- Guidelines on Personal data breach notification under Regulation 2016/679 - 6 febbraio 2018

2.4.1.3. Opinioni

- WP266 Opinion on Commission proposals on establishing a framework for interoperability
- Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC) - wp247
- Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), wp258
- Opinion 2/2017 on data processing at work - wp249
- Opinion 04/2016 on European Commission amendments proposals related to the powers of Data Protection Authorities in Standard Contractual Clauses and adequacy decisions - wp241

2.4.1.4. Lettere e altri documenti

- List of companies for which the EU BCR cooperation procedure is closed
- Position Paper related to article 30(5)
- Recommendation on the approval of the Controller Binding Corporate Rules form (wp264)
- Recommendation on the approval of the Processor Binding Corporate Rules form (wp265)
- Working Document on the approval procedure of the Binding Corporate Rules for controllers and processors (wp263rev.01)
- Article 29 WP Statement on encryption (ePrivacy)
- Working Document on Binding Corporate Rules for Processors (wp257rev.01)
- Working Document on Binding Corporate Rules for Controllers (wp256rev.01)
- Working document on Adequacy Referential (wp254rev.01)

2.4.2. Linee guida Commission Nationale de l'Informatique et des Libertés (CNIL)

- Methodology for Privacy Risk Management - Translation of June 2012 edition

3. QUADRO NORMATIVO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Il presente capitolo è dedicato a esporre e interpretare la normativa vigente in ambito di trattamento dei dati personali.

Ogni paragrafo è diviso in due sezioni: una riporta “Cosa dice la normativa” e l’altra ne fornisce una interpretazione.

La sezione “Cosa dice la normativa” contiene testi che sono stati rielaborati al fine di offrire una più facile lettura e comprensione a tutte le tipologie di lettori. Pertanto può non essere esaustiva: in caso di dubbi o esigenze particolari e complesse si consiglia di rivolgersi a consulenti esperti in ambito privacy.

Quando non diversamente indicato, gli articoli si riferiscono al Regolamento.

3.1. Art.4: Definizioni

3.1.1. Che cosa dice la normativa

Si riportano le definizioni utili alla comprensione del documento estratte dal Regolamento e dal Decreto 101/2018.

Termine	*Definizione*	*Origine*
archivio	qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico	Regolamento Art.4
comunicazione	il dare conoscenza dei dati personali a uno o piu' soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione	Decreto 101/2018 (art. 2-ter)
comunicazione elettronica	ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come	Decreto 101/2018 (art. 121)

	parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un contraente o utente ricevente, identificato o identificabile	
consenso dell'interessato	qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;	Regolamento Art.4
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;	Regolamento Art.4
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;	Regolamento Art.4
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;	Regolamento Art.4
dato anonimo	dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile	Decreto 101/2018
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;	Regolamento Art.4
destinatario	la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto	Regolamento Art.4

	dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;	
diffusione	il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione	Decreto 101/2018 (art. 2-ter)
garante della privacy	l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.	Decreto 101/2018
incaricati	le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;	Decreto 101/2018
interessato	la persona fisica cui si riferiscono i dati personali	Decreto 101/2018
limitazione di trattamento	il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro	Regolamento Art.4
profilazione	qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica	Regolamento Art.4
profilo di autorizzazione	l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;	Decreto 101/2018
pseudonimizzazione	il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile	Regolamento Art.4
responsabile del trattamento	la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento	Regolamento Art.4

sistema di autorizzazione	l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente	Decreto 101/2018
stabilimento principale	per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale; con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente Regolamento;	Regolamento Art.4
strumenti elettronici	gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;	Decreto 101/2018
terzo	la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile	Regolamento Art.4
titolare del trattamento	la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;	Regolamento Art.4
trattamento	qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi	Regolamento Art.4

	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	
trattamento transfrontaliero	trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;	Regolamento Art.4
utente	qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali	Decreto 101/2018
violazione dei dati personali	la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;	Regolamento Art.4
violazione di dati personali	violazione della sicurezza che comporta anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico.	Decreto 101/2018

3.2. Ambito di applicazione del Regolamento

3.2.1. Che cosa dice la normativa

3.2.1.1. Art.2: Ambito di applicazione materiale

Articolo 2 del Regolamento

1. Il presente regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.

2. Il presente regolamento **non si applica ai trattamenti di dati personali**:

a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;
b) effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE, ovvero politica estera e sicurezza comune nell'Unione Europea;
c) **effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico**;
d) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

3. *Omissis*

4. *Omissis*

3.2.1.2. Art.3: Ambito di applicazione territoriale

Articolo 3 del Regolamento

1. Il presente regolamento **si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione**, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.

2. Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:

a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure
b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

3. Il presente regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico.

3.2.2. Interpretazioni

Il Regolamento si applica al trattamento (sia interamente, che parzialmente che non automatizzato) di dati personali contenuti in un qualsiasi archivio o destinati a figurarvi.

Il Regolamento **disciplina** il trattamento dei dati personali

- **delle persone fisiche**, a prescindere dalla nazionalità o dal luogo di residenza, in relazione al trattamento dei loro dati personali (considerando 14)

Il Regolamento **non disciplina** il trattamento dei dati personali

- relativi a **persone giuridiche**, in particolare imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto (considerando 14);
- effettuato da una persona fisica nell'ambito di **attività a carattere esclusivamente personale o domestico** e quindi senza una connessione con un'attività commerciale o professionale; tali attività potrebbero comprendere la corrispondenza e gli indirizzari, o l'uso dei social network e attività online intraprese nel quadro di tali attività. (considerando 18);
- relativi a **persone decedute** (considerando 27), ad **esclusione** di quanto specificato nell'articolo 2-terdecies del Decreto 101/2018 (vedi 3.4.1.11. Art. 2-terdecies del Decreto 101/2018: Diritti riguardanti le persone decedute).

Relativamente all'ambito territoriale, il Regolamento disciplina il trattamento dei dati personali

- **quando il titolare o responsabile** del trattamento **è stabilito nell'Unione Europea**, a prescindere dal fatto che il trattamento sia effettuato o meno nell'Unione Europea,
- Se i dati personali sono relativi ad **interessati che si trovano nell'Unione**, a prescindere dal fatto che **il titolare del trattamento o il responsabile del trattamento sia stabilito nell'Unione**, quando le attività di trattamento riguardano:
    - l'**offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione Europea**, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure
    - il **monitoraggio del loro comportamento** nella misura in cui tale comportamento **ha luogo all'interno dell'Unione Europea**.

3.3. Principi

3.3.1. Che cosa dice la normativa

3.3.1.1. Art.5: Principi applicabili al trattamento di dati personali

Articolo 5 del Regolamento

1. I dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (**«liceità, correttezza e trasparenza»**);
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali (**«limitazione della finalità»**);
c) c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (**«minimizzazione dei dati»**);
d) d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati **(«esattezza»**);

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato (**«limitazione della conservazione»**);
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (**«integrità e riservatezza»**).

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

3.3.1.2. Art.6: Liceità del trattamento

Articolo 6 del Regolamento

1. Il **trattamento è lecito** solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il **consenso** al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è **necessario all'esecuzione di un contratto** di cui l'interessato è parte o all'esecuzione di **misure precontrattuali** adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un **obbligo legale** al quale è soggetto il titolare del trattamento;
d) il trattamento è necessario per la **salvaguardia degli interessi vitali** dell'interessato o di un'altra persona fisica;
e) il trattamento è necessario per l'**esecuzione di un compito di interesse pubblico** o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
f) il trattamento è necessario per il **perseguimento del legittimo interesse del titolare del trattamento o di terzi**, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore. La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

2. *Omissis*

3. *Omissis*

4. Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri *omissis*, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro:

a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;

b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento;
c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9 (vedi 3.3.1.6. Art.9: Trattamento di categorie particolari di dati personali), oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10 (vedi 3.3.1.7. Art.10: Trattamento di dati personali relativi a condanne penali e reati);
d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;
e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

3.3.1.3. Art. 130 del Decreto 101/2018: Comunicazioni indesiderate

1. Fermo restando quanto stabilito dagli articoli 8 e 21 del decreto legislativo 9 aprile 2003, n. 70, l'uso di **sistemi automatizzati** di chiamata o di comunicazione di chiamata **senza l'intervento di un operatore** per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di **comunicazione commerciale è consentito con il consenso del contraente o utente**. Resta in ogni caso fermo quanto previsto dall'articolo 1, comma 14, della legge 11 gennaio 2018, n. 5.

2. La disposizione di cui al comma 1 si applica anche alle **comunicazioni elettroniche, effettuate per le finalità ivi indicate, mediante posta elettronica**, telefax, messaggi del tipo Mms (Multimedia Messaging Service) o Sms (Short Message Service) o di altro tipo.

3. Fuori dei casi di cui ai commi 1 e 2, ulteriori comunicazioni per le finalità di cui ai medesimi commi effettuate con mezzi diversi da quelli ivi indicati, sono consentite ai sensi degli articoli 6 (vedi 3.3.1.2. Art.6: Liceità del trattamento) e 7 (vedi 3.3.1.3. Art.7: Condizioni per il consenso) del Regolamento nonché ai sensi di quanto previsto dal comma 3-bis.

3-bis. *Omissis*

3-ter. *Omissis*

3-quater. *Omissis*

4. (*n.d.r. attività di soft-spam*) Fatto salvo quanto previsto nel comma 1, **se il titolare del trattamento utilizza, a fini di vendita diretta di propri prodotti o servizi, le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio, può non richiedere il consenso dell'interessato, sempre che si tratti di servizi analoghi a quelli oggetto della vendita** e l'interessato, adeguatamente informato, non rifiuti tale uso, inizialmente o in occasione di successive comunicazioni. L'interessato, al momento della raccolta e in occasione dell'invio di ogni comunicazione effettuata per le finalità di cui al presente comma, è informato della possibilità di opporsi in ogni momento al trattamento, in maniera agevole e gratuitamente.

5. È vietato in ogni caso l'invio di comunicazioni per le finalità di cui al comma 1 o, comunque, a scopo promozionale, effettuato camuffando o celando l'identità del mittente o in violazione dell'articolo 8 del decreto legislativo 9 aprile 2003, n. 70, o senza fornire un idoneo recapito presso il quale l'interessato possa esercitare i diritti di cui agli articoli da 15 a 22 (vedi 3.4. Diritti dell'interessato) del Regolamento, oppure esortando i destinatari a visitare siti web che violino il predetto articolo 8 del decreto legislativo n. 70 del 2003.

6. In caso di reiterata violazione delle disposizioni di cui al presente articolo il Garante può, provvedendo ai sensi dell'articolo 58 (vedi 3.10.1.3. Art.58: Poteri dell'autorità di controllo) del Regolamento altresì prescrivere a fornitori di servizi di comunicazione elettronica di adottare procedure di filtraggio o altre misure praticabili relativamente alle coordinate di posta elettronica da cui sono stati inviate le comunicazioni.

3.3.1.4. Art.7: Condizioni per il consenso

Articolo 7 del Regolamento

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

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

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

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

3.3.1.5. Art.8: Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione

Articolo 8 del Regolamento

1. Qualora si applichi l'articolo 6 (vedi 3.3.1.2. Art.6: Liceità del trattamento), paragrafo 1, lettera a) (*n.d.r. l'interessato ha espresso il consenso al trattamento*), per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.

Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni.

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

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

3.3.1.6. Art. 2-quinquies del Decreto 101/2018: consenso del minore in relazione ai servizi della società dell'informazione

Articolo 2-quinquies del Decreto 101/2018

1. In attuazione dell'articolo 8 (vedi 3.3.1.4. Art.8: Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione), paragrafo 1, del Regolamento, il minore che ha compiuto i quattordici anni puo' esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della societa' dell'informazione. Con riguardo a tali servizi, il trattamento dei dati personali del minore di eta' inferiore a quattordici anni, fondato sull'articolo 6 (vedi 3.3.1.2. Art.6: Liceità del trattamento), paragrafo 1, lettera a) (*n.d.r. L'interessato ha espresso il consenso*), del Regolamento, e' lecito a condizione che sia prestato da chi esercita la responsabilita' genitoriale.

2. In relazione all'offerta diretta ai minori dei servizi di cui al comma 1, il titolare del trattamento redige con linguaggio particolarmente chiaro e semplice, conciso ed esaustivo, facilmente accessibile e comprensibile dal minore, al fine di rendere significativo il consenso prestato da quest'ultimo, le informazioni e le comunicazioni relative al trattamento che lo riguardi.

3.3.1.7. Art.9: Trattamento di categorie particolari di dati personali

Articolo 9 del Regolamento

1. È vietato trattare **dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona**.

2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi (*n.d.r. è lecito trattare particolari categorie di dati personali*):

a) l'interessato **ha prestato il proprio consenso esplicito** al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1;
b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di **diritto del lavoro e della sicurezza sociale e protezione sociale**, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;
c) il trattamento è necessario per **tutelare un interesse vitale** dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
d) *omissis*;
e) il trattamento riguarda **dati personali resi manifestamente pubblici** dall'interessato;

f) il trattamento è necessario per accertare, esercitare o difendere un **diritto in sede giudiziaria** o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
g) il trattamento è necessario per **motivi di interesse pubblico** rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;
h) il trattamento è necessario per finalità di **medicina preventiva o di medicina del lavoro**, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3;
i) *omissis*;
j) *omissis*.

3. I dati personali di cui al paragrafo 1 possono essere trattati per le finalità di cui al paragrafo 2, lettera h) (*n.d.r. finalità di medicina preventiva o di medicina del lavoro*), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti.

4. Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute.

3.3.1.8. Art.10: Trattamento di dati personali relativi a condanne penali e reati

Articolo 10 del Regolamento

Il trattamento dei dati personali relativi a condanne penali e reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1 (vedi 3.3.1.2. Art.6: Liceità del trattamento) **deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal** diritto dell'Unione o **degli Stati membri (**vedi 3.3.1.9. Art. 2-octies del Decreto 101/2018: Principi relativi al trattamento di dati relativi a condanne penali e reati) che preveda garanzie appropriate per i diritti e le libertà degli interessati.
Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.

3.3.1.9. Art. 2-octies del Decreto 101/2018: Principi relativi al trattamento di dati relativi a condanne penali e reati

Articolo 2-octies del Decreto 101/2018

1. Fatto salvo quanto previsto dal decreto legislativo 18 maggio 2018, n. 51, il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza sulla base dell'articolo 6 (vedi 3.3.1.2. Art.6: Liceità del trattamento), paragrafo 1, del Regolamento, che non avviene sotto il controllo dell'autorità pubblica, e' consentito, ai sensi dell'articolo 10 (vedi 3.3.1.7. Art.10: Trattamento di dati personali relativi a condanne penali e reati) del medesimo

regolamento, solo se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, che prevedano garanzie appropriate per i diritti e le liberta' degli interessati.

2. In mancanza delle predette disposizioni di legge o di regolamento, i trattamenti dei dati di cui al comma 1 nonche' le garanzie di cui al medesimo comma sono individuati con decreto del Ministro della giustizia, da adottarsi, ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, sentito il Garante.

3. Fermo quanto previsto dai commi 1 e 2, **il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza e' consentito** se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, riguardanti, in particolare:

a) **l'adempimento di obblighi e l'esercizio di diritti da parte del titolare o dell'interessato in materia di diritto del lavoro o comunque nell'ambito dei rapporti di lavoro**, nei limiti stabiliti da leggi, regolamenti e contratti collettivi, secondo quanto previsto dagli articoli 9, paragrafo 2, lettera b), e 88 del regolamento;
b) **l'adempimento degli obblighi previsti da disposizioni di legge o di regolamento in materia di mediazione finalizzata alla conciliazione delle controversie civili e commerciali**;
c) **la verifica o l'accertamento dei requisiti di onorabilita', requisiti soggettivi e presupposti interdittivi nei casi previsti dalle leggi o dai regolamenti**;
d) **l'accertamento di responsabilita' in relazione a sinistri o eventi attinenti alla vita umana, nonchè la prevenzione, l'accertamento e il contrasto di frodi o situazioni di concreto rischio per il corretto esercizio dell'attivita' assicurativa**, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia;
e) **l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria**;
f) **l'esercizio del diritto di accesso ai dati e ai documenti amministrativi**, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia;
g) l**'esecuzione di investigazioni o le ricerche o la raccolta di informazioni per conto di terzi** ai sensi dell'articolo 134 del testo unico delle leggi di pubblica sicurezza;
h) *omissis*, o per la produzione della **documentazione prescritta dalla legge per partecipare a gare d'appalto**;
i) l'accertamento del **requisito di idoneità morale di coloro che intendono partecipare a gare d'appalto**, in adempimento di quanto previsto dalle vigenti normative in materia di appalti;
j) *omissis*,
k) *omissis*.

4. Nei casi in cui le disposizioni di cui al comma 3 non individuano le garanzie appropriate per i diritti e le liberta' degli interessati, tali garanzie sono previste con il decreto di cui al comma 2.

5. *Omissis*.

6. *Omissis*.

3.3.1.10. Art.11: Trattamento che non richiede l'identificazione

Articolo 11 del Regolamento

1. Se le finalità per cui un titolare del trattamento tratta i dati personali non richiedono o non richiedono più l'identificazione dell'interessato, il titolare del trattamento non è obbligato a

conservare, acquisire o trattare ulteriori informazioni per identificare l'interessato al solo fine di rispettare il presente regolamento.

2. Qualora, nei casi di cui al paragrafo 1 del presente articolo, il titolare del trattamento possa dimostrare di non essere in grado di identificare l'interessato, ne informa l'interessato, se possibile. In tali casi, gli articoli da 15 a 20 (vedi 3.4.1.2. Art.15: Diritto di Accesso, 3.4.1.3. Art.16: Diritto di rettifica, 3.4.1.4. Art.17: Diritto alla cancellazione («diritto all'oblio»), 3.4.1.4. Art.17: Diritto alla cancellazione («diritto all'oblio»), 3.4.1.5. Art.18: Diritto di limitazione di trattamento, 3.4.1.7. Art.20: Diritto alla portabilità dei dati) non si applicano tranne quando l'interessato, al fine di esercitare i diritti di cui ai suddetti articoli, fornisce ulteriori informazioni che ne consentano l'identificazione.

3.3.2. Interpretazioni

3.3.2.1. Principi generali

Al principio di responsabilizzazione, di particolare rilevanza, è dedicato l'approfondimento 8.3. Principio di responsabilizzazione o "accountability".

3.3.2.2. Liceità del trattamento

In generale risulta lecito trattare dati personali se l'interessato ha prestato il proprio **consenso esplicito al trattamento.** Tuttavia esistono delle condizioni che rendono non necessaria la richiesta di consenso. Particolarmente pertinenti risultano le seguenti.

1. 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. Per esempio i dati personali relativi ad un cliente che servono per instaurare un contratto, o all'esecuzione del un contratto possono essere trattati senza il consenso esplicito dell'interessato.
2. Il **trattamento è necessario per adempiere un obbligo legale** al quale è soggetto il titolare del trattamento.
3. Il **trattamento è necessario per la salvaguardia degli interessi vitali** dell'interessato o di un'altra persona fisica. Ad esempio è lecito trattare dati di contatto dell'interessato o di suoi parenti a fini di soccorso immediato di un infortunato.
4. 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.
5. 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. In base al considerando 47, ad esempio, potrebbero sussistere tali legittimi interessi quando **l'interessato è un cliente o è alle dipendenze del titolare del trattamento**. Costituisce parimenti legittimo interesse del titolare del trattamento interessato trattare dati personali strettamente necessari a fini di **prevenzione delle frodi**. La citazione contenuta nel considerando 47 "Può essere considerato legittimo interesse trattare dati personali per finalità di **marketing diretto**" risulta invece in contrasto con quanto stabilito dal articolo 130 del Decreto 101/2018 (vedi 3.3.1.3. Art. 130 del Decreto 101/2018: Comunicazioni indesiderate), pertanto **si faccia**

riferimento alle disposizioni dell' articolo 130 del Decreto 101/2018 per quanto concerne le comunicazioni commerciali, come ad esempio l'invio di newsletters.

È lecito trattare i **dati per una finalità diversa da quella per cui sono stati raccolti** solo se i sono stati raccolti sulla base di un **interesse legittimo**, di un **contratto** o di **interessi vitali**, e solo se **la nuova finalità è compatibile con quella originaria**.

N**on è dunque lecito trattare dati per una finalità diversa** da quella per cui sono stati raccolti se i dati sono stati raccolti sulla base del **consenso** dell'interessato.

In base al considerando 50, per accertare se la finalità di un ulteriore trattamento sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento dovrebbe, dopo aver soddisfatto tutti i requisiti per la liceità del trattamento originario, tener conto

- di ogni nesso tra tali finalità e le finalità dell'ulteriore trattamento previsto,
- del contesto in cui i dati personali sono stati raccolti, in particolare le ragionevoli aspettative dell'interessato in base alla sua relazione con il titolare del trattamento con riguardo al loro ulteriore utilizzo;
- della natura dei dati personali; delle conseguenze dell'ulteriore trattamento previsto per gli interessati;
- dell'esistenza di garanzie adeguate sia nel trattamento originario sia nell'ulteriore trattamento previsto.

In ogni caso, dovrebbe essere garantita l'applicazione dei principi stabiliti dal presente regolamento, in particolare l'obbligo di informare l'interessato di tali altre finalità e dei suoi diritti, compreso il diritto di opporsi.

3.3.2.3. Condizioni per il consenso

In base alle definizioni (vedi 3.1. Art.4: Definizioni) il consenso è 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.

L'espressione del consenso deve essere libera. **Non si può considerare libero**, e quindi valido, un consenso

- espresso da un interessato che **non ha reale scelta** o che si sente costretto,
- che potrebbe procurare **conseguenze negative se non dato**,
- legato ad una **parte non negoziabile di termini e condizioni di un contratto**,
- che l'interessato non può revocare senza subire danno.

L'espressione del consenso deve essere specifica. Ovvero **il consenso deve essere dato in relazione a una o più finalità specifiche**. Ciò è strettamente legato alla liceità del trattamento: indipendentemente dalle modalità, trattamento risulta lecito solo se, in caso sia basato sul consenso, sia effettuato per le finalità specifiche per le quali è stato espresso il consenso (vedi 3.3.1.3. Art.7: Condizioni per il consenso).

L'espressione del consenso deve essere informata. In base al principio di trasparenza, il consenso può essere richiesto solo dopo avere adeguatamente informato l'interessato in modo che possa effettuare una scelta consapevole, diversamente il consenso non risulta valido per procedere al trattamento. A tal fine le informazioni fornite devono essere comprensibili dall'interessato, espresse in un linguaggio familiare all'interessato, facilmente leggibili in particolare se incluse all'interno di un contratto.

Per ottenere un consenso valido, all'interessato dovrebbero essere fornite almeno le seguenti informazioni:

1. identità del titolare,
2. finalità di ciascun trattamento per il quale si richiede il consenso,
3. categorie di dati raccolti e trattati,
4. esistenza del diritto alla revoca del consenso,
5. eventuale utilizzo di processi decisionali automatizzati (descritti nel paragrafo 3.4.1.9. Art.22: Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione),
6. eventuali rischi derivanti da trasferimenti in paesi extra UE in assenza delle decisioni di adeguatezza e garanzie adeguate.

Tali **informazioni sono un sottoinsieme di** quelle descritte nel paragrafo 3.4.1.1. Art.12,13,14: Informazioni all'interessato relative al trattamento dei dati personali, dette comunemente ***informativa sul trattamento dei dati personali***, ovvero le informazioni da fornire all'interessato relativamente al trattamento dei dati personali, indipendentemente dalla necessità di ottenere o meno il consenso al trattamento.

Pertanto se si richiede il consenso contestualmente alla comunicazione della informativa, è sufficiente integrare le informazioni con

- le finalità per cui verranno trattati i dati che richiedono il consenso: qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste,
- le conseguenze derivanti dal mancato consenso al trattamento (sempre tenendo conto dei requisiti affinchè un consenso si possa considerare liberamente prestato sopra descritti),
- l'esistenza del diritto alla revoca del consenso,
- formula di dichiarazione di consenso.

In base al considerando 32, il **consenso dovrebbe essere espresso mediante un atto positivo inequivocabile** con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Tuttavia il titolare, nel scegliere la modalità di espressione del consenso, deve tenere conto del fatto che in base al principio di responsabilizzazione deve poter dimostrare di avere ottenuto il consenso al trattamento dall'interessato.

Il consenso potrebbe dunque essere espresso attraverso la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto.

Non dovrebbe configurare consenso il silenzio, l'inattività o la preselezione di caselle.

3.3.2.4. Trattamento di particolari categorie di dati personali

Per particolari categorie di dati personali si intendono

- dati personali che rivelino l'origine razziale o etnica,
- dati personali che rivelino le opinioni politiche,
- dati personali che rivelino le convinzioni religiose o filosofiche,
- dati personali che rivelino l'appartenenza sindacale,
- dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica,
- dati relativi alla salute,
- dati relativi alla vita sessuale o all'orientamento sessuale

della persona.

Esempi di categorie particolari di dati personali sono forniti nell' approfondimento 8.1. Dati personali, particolari categorie di dati personali e dati personali relativi a condanne penali e reati.

In base al considerando 51, le **categorie particolari di dati personali** meritano una specifica protezione in quanto sono dati personali, per loro natura, particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, dal momento che il contesto del loro trattamento potrebbe creare **rischi significativi per i diritti e le libertà fondamentali**.

Pertanto, in generale risulta lecito trattare particolari categorie di dati personali se l'interessato ha prestato il proprio **consenso esplicito al trattamento.**

Tuttavia esistono delle condizioni che rendono **non necessaria la richiesta di consenso**. Particolarmente pertinenti risultano le seguenti.

1. Il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato **in materia di diritto del lavoro**. Ad esempio non è necessario richiedere il consenso per trattare i dati relativi assenze per malattia, certificati e visite mediche, documentazione relativa alla gravidanza, ecc..
2. Il trattamento è necessario per **tutelare un interesse vitale** dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso. Se ad esempio è lecito trattare informazioni relative allo stato di salute a fini di soccorso immediato di un infortunato, anche se l'infortunato è nell'impossibilità di prestare il proprio consenso.
3. Il trattamento riguarda dati personali resi **manifestamente pubblici** dall'interessato.
4. Il trattamento è necessario per finalità di **medicina preventiva o di medicina del lavoro**.I dati devono essere trattati da o sotto la responsabilità di un **professionista soggetto al segreto professionale**. Ad esempio non è necessario richiedere il consenso per valutazione dell'idoneità alla mansione lavorativa e finalità connesse.

3.3.2.5. Trattamento di dati personali relativi a condanne penali e reati

Con riferimento ai dati personali relativi a condanne penali e reati è opportuno precisare che tipicamente uno studio o un libero professionista che opera in ambito non legale, si trova a trattare dati di questo tipo principalmente in questi casi:

- svolgimento di attività di mediazione finalizzata alla conciliazione delle controversie civili e commerciali;

- partecipazione a gare o appalti pubblici per i quali è prescritta dalla legge la presentazione documentazione specifica, come ad esempio il "Casellario giudiziale" di Amministratori e/o Direttori tecnici delle Società partecipanti alla gara, ed in alcuni casi di Mandanti e Mandatarie;
- svolgimento di incarichi in qualità di Consulente Tecnico d'Ufficio (CTU) o Consulente Tecnico di Parte (CTP).

Il trattamento di dati relativi a condanne penali e reati nelle **attività di mediazione e per la partecipazione a gare d'appalto** è esplicitamente consentito dal comma 3 dell'articolo 2-octies del Decreto 101/2018 (vedi 3.3.1.8. Art. 2-octies del Decreto 101/2018: Principi relativi al trattamento di dati relativi a condanne penali e reati).

Per le attività svolte come in qualità di **Consulente Tecnico d'Ufficio (CTU) o Consulente Tecnico di Parte (CTP)** si rimanda all'approfondimento 8.3. Trattamento di dati personali nel ruolo di CTU e CTP.

Definizioni ed esempi di dati relativi a condanne penali e reati sono disponibili nell' approfondimento 8.1. Dati personali, particolari categorie di dati personali e dati personali relativi a condanne penali e reati.

3.4. Diritti dell'interessato

3.4.1. Cosa dice la normativa

3.4.1.1. Art.13,14 del Regolamento e Art.111-bis del Decreto 101/2018: Informazioni all'interessato relative al trattamento dei dati personali

Articolo 13 del Regolamento: Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato

1. In caso di **raccolta presso l'interessato** di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:

a) l'identità e i dati di contatto del **titolare del trattamento** e, ove applicabile, del suo rappresentante;
b) i dati di contatto del **responsabile della protezione dei dati**, ove applicabile;
c) le **finalità del trattamento** cui sono destinati i dati personali nonché la base giuridica del trattamento;
d) qualora il trattamento si basi sull'articolo 6 (vedi 3.3.1.2. Art.6: Liceità del trattamento), paragrafo 1, lettera f) (*n.d.r. legittimo interesse*), **i legittimi interessi perseguiti dal titolare del trattamento o da terzi**;
e) gli **eventuali destinatari** o le eventuali categorie di destinatari dei dati personali;
f) ove applicabile, l'intenzione del titolare del trattamento di **trasferire dati personali a un paese terzo** o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 (vedi 3.6.1.3. Art.46: Trasferimento soggetto a garanzie adeguate) o 47 (*n.d.r. norme vincolanti d'impresa*), o all'articolo 49 (vedi 3.6.1.4. Art.47: Norme vincolanti d'impresa), paragrafo 1, secondo comma, il riferimento alle garanzie appropriate o

opportune e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili.

2. In aggiunta alle informazioni di cui sopra, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti **ulteriori informazioni** necessarie per garantire un trattamento corretto e trasparente:

a) il **periodo di conservazione** dei dati personali oppure, se non è possibile, i **criteri utilizzati per determinare tale periodo**;
b) l'**esistenza del diritto** dell'interessato di chiedere al titolare del trattamento **l'accesso** ai dati personali e la **rettifica** o la **cancellazione** degli stessi o la **limitazione del trattamento** che lo riguardano o di **opporsi** al loro trattamento, oltre al **diritto alla portabilità dei dati**;
c) qualora il trattamento sia basato sull'articolo 6 (vedi 3.3.1.2. Art.6: Liceità del trattamento), paragrafo 1, lettera a) (*n.d.r. consenso al trattamento di dati personali*), oppure sull'articolo 9 (vedi 3.3.1.6. Art.9: Trattamento di categorie particolari di dati personali), paragrafo 2, lettera a) (*n.d.r. consenso al trattamento di particolari categorie di dati personali*), l'**esistenza del diritto di revocare il consenso** in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
d) il **diritto** di proporre **reclamo** a un'autorità di controllo;
e) **se** la comunicazione di dati personali è un **obbligo legale o contrattuale** oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili **conseguenze della mancata comunicazione di tali dati**;
f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22 (vedi 3.4.1.9. Art.22: Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione), paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

3. Qualora il titolare del trattamento intenda **trattare ulteriormente i dati personali per una finalità diversa** da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2.

4. I paragrafi 1, 2 e 3 non si applicano se e nella misura in cui l'interessato dispone già delle informazioni.

Articolo 14 del Regolamento: Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato

1. Qualora i **dati non siano stati ottenuti presso l'interessato**, il titolare del trattamento **fornisce all'interessato** le seguenti informazioni:

a) l'identità e i dati di contatto del **titolare del trattamento** e, ove applicabile, del suo rappresentante;
b) i dati di contatto del **responsabile della protezione dei dati**, ove applicabile;

c) le **finalità del trattamento** cui sono destinati i dati personali nonché la base giuridica del trattamento;
d) le **categorie di dati personali** in questione;
e) gli **eventuali destinatari** o le eventuali categorie di destinatari dei dati personali;
f) ove applicabile, l'intenzione del titolare del trattamento di **trasferire dati personali a un paese terzo** o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 (vedi 3.6.1.3. Art.46: Trasferimento soggetto a garanzie adeguate) o 47 (*n.d.r. norme vincolanti d'impresa*), o all'articolo 49 (vedi 3.6.1.4. Art.47: Norme vincolanti d'impresa), paragrafo 1, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili.

2. Oltre alle informazioni di cui al paragrafo 1, il titolare del trattamento fornisce all'interessato le seguenti informazioni necessarie per garantire un trattamento corretto e trasparente nei confronti dell'interessato:

a) il **periodo di conservazione** dei dati personali oppure, se non è possibile, i **criteri utilizzati per determinare tale periodo**;
b) qualora il trattamento si basi sull'articolo 6 (vedi 3.3.1.2. Art.6: Liceità del trattamento), paragrafo 1, lettera f) *(n.d.r. legittimo interesse*), **i legittimi interessi perseguiti dal titolare del trattamento o da terzi**;
c) l'esistenza del **diritto** dell'interessato di chiedere al titolare del trattamento **l'accesso** ai dati personali e la **rettifica** o la **cancellazione** degli stessi o la **limitazione del trattamento** dei dati personali che lo riguardano e di **opporsi** al loro trattamento, oltre al diritto alla **portabilità dei dati**;
d) qualora il trattamento sia basato sul consenso, l'esistenza del **diritto** di **revocare il consenso** in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca;
e) il **diritto** di proporre **reclamo** a un'autorità di controllo;
f) la **fonte da cui hanno origine i dati personali** e, se del caso, **l'eventualità** che i dati provengano da **fonti accessibili al pubblico**;
g) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22 (vedi 3.4.1.9. Art.22: Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione), paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

4. Qualora il titolare del trattamento intenda t**rattare ulteriormente i dati personali per una finalità diversa** da quella per cui essi sono stati ottenuti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni informazione pertinente di cui al paragrafo 2.

5. I paragrafi da 1 a 4 non si applicano (*n.d.r. il titolare è esonerato dal comunicare le informazioni all'interessato*) se e nella misura in cui:

a) l'interessato **dispone già delle informazioni**;
b) comunicare tali informazioni risulta impossibile o implicherebbe uno **sforzo sproporzionato**; *omissis*;

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

Art. 111-bis del Decreto 101/2018: Informazioni in caso di ricezione di curriculum

1. Le **informazioni** di cui all'articolo 13 del Regolamento, **nei casi di ricezione dei curricula spontaneamente trasmessi dagli interessati** al fine della instaurazione di un rapporto di lavoro, vengono fornite **al momento del primo contatto** utile, successivo all'invio del curriculum medesimo. Nei limiti delle finalità di cui all'articolo 6 (vedi 3.3.1.2. Art.6: Liceità del trattamento), paragrafo 1, lettera b), del Regolamento (*n.d.r. il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso*), **il consenso al trattamento dei dati personali presenti nei curricula non è dovuto**.

3.4.1.2. Art.15: Diritto di Accesso

Articolo 15 del Regolamento

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di **ottenere l'accesso ai dati personali** e alle seguenti informazioni:

a) le finalità del trattamento;
b) le categorie di dati personali in questione;
c) i 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;
d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
e) l'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;
f) il diritto di proporre reclamo a un'autorità di controllo;
g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22 (vedi 3.4.1.9. Art.22: Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione), paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

2. Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 (vedi 3.6.1.3. Art.46: Trasferimento soggetto a garanzie adeguate) relative al trasferimento.

3. **Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento**. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un

contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

4. Il diritto di ottenere una copia di cui al paragrafo 3 **non deve ledere i diritti e le libertà altrui**.

3.4.1.3. Art.16: Diritto di rettifica

Articolo 16 del Regolamento

L'interessato ha il diritto di ottenere dal titolare del trattamento la **rettifica dei dati personali inesatti** che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

3.4.1.4. Art.17: Diritto alla cancellazione («diritto all'oblio»)

Articolo 17 del Regolamento

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la **cancellazione dei dati personali** che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, **se** sussiste uno dei motivi seguenti:

a) i **dati personali non sono più necessari** rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
b) l'interessato **revoca il consenso** su cui si basa il trattamento conformemente all'articolo 6 (vedi 3.3.1.2. Art.6: Liceità del trattamento), paragrafo 1, lettera a) (*n.d.r. consenso al trattamento dei dati personali*), o all'articolo 9 (vedi 3.3.1.6. Art.9: Trattamento di categorie particolari di dati personali), paragrafo 2, lettera a) *(n.d.r. consenso al trattamento di particolari categorie di dati personali*), e se non sussiste altro fondamento giuridico per il trattamento;
c) l'interessato si **oppone al trattamento** ai sensi dell'articolo 21 (vedi 3.4.1.8. Art.21: Diritto di opposizione), paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;
d) i dati personali sono stati **trattati illecitamente**;
e) i dati personali devono essere cancellati per adempiere un **obbligo giuridico** previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
f) *omissis*.

2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

3. I paragrafi 1 e 2 non si applicano (*n.d.r.* ***il diritto alla cancellazione non è esercitabile***) nella misura in cui il **trattamento sia necessario**:

a) per l'esercizio del diritto alla **libertà di espressione e di informazione**;

b) per l'**adempimento di un obbligo legale** che richieda il trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
c) per **motivi di interesse pubblico** nel settore della **sanità pubblica** *omissis*;
d) a fini di **archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici** *omissis*; o
e) per l'accertamento, l'esercizio o la difesa di un **diritto in sede giudiziaria**.

3.4.1.5. Art.18: Diritto di limitazione di trattamento

Articolo 18 del Regolamento

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la **limitazione del trattamento** 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 (vedi 3.4.1.8. Art.21: Diritto di opposizione), paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

2. Se il **trattamento è limitato** a norma del paragrafo 1, tali **dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico** *omissis*.

3. L'interessato che ha ottenuto la limitazione a norma del paragrafo 1 del trattamento è informato dal titolare del trattamento prima che detta limitazione sia revocata.

3.4.1.6. Art.19: Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento

Articolo 19 del Regolamento

Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma dell'articolo 16 (vedi 3.4.1.3. Art.16: Diritto di rettifica), dell'articolo 17 (vedi 3.4.1.4. Art.17: Diritto alla cancellazione («diritto all'oblio»)), paragrafo 1, e dell'articolo 18 (vedi 3.4.1.5. Art.18: Diritto di limitazione di trattamento), salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

3.4.1.7. Art.20: Diritto alla portabilità dei dati

Articolo 20 del Regolamento

1. L'interessato ha il **diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali** che lo riguardano forniti a un titolare del trattamento e ha il diritto di **trasmettere tali dati a un altro titolare** del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:

a) il trattamento si basi sul consenso ai sensi dell'articolo 6 (vedi 3.3.1.2. Art.6: Liceità del trattamento), paragrafo 1, lettera a) (*n.d.r. consenso al trattamento dei dati personali*), o dell'articolo 9 (vedi 3.3.1.6. Art.9: Trattamento di categorie particolari di dati personali), paragrafo 2, lettera a) (*n.d.r. consenso al trattamento di particolari categorie di dati personali*), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e
b) il trattamento sia effettuato con mezzi automatizzati.

2. Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.

3. L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17 (vedi 3.4.1.4. Art.17: Diritto alla cancellazione («diritto all'oblio»)). Tale diritto non si applica al trattamento 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.

4. Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui.

3.4.1.8. Art.21: Diritto di opposizione

Articolo 21 del Regolamento

1. L'interessato ha il **diritto di opporsi in qualsiasi momento**, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6 (vedi 3.3.1.2. Art.6: Liceità del trattamento), paragrafo 1, lettere e) (*n.d.r. trattamento necessario per l'esecuzione di un compito di interesse pubblico*) o f) (*n.d.r. trattamento necessario per il perseguimento del legittimo interesse*), compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

2. Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.

3. Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità.

4. Il diritto di cui ai paragrafi 1 e 2 è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.

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

6. *Omissis*

3.4.1.9. Art.22: Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione

Articolo 22 del Regolamento

1. L'interessato ha il **diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona**.

2. Il paragrafo 1 **non si applica** nel caso in cui la decisione:

a) sia **necessaria per la conclusione o l'esecuzione di un contratto** tra l'interessato e un titolare del trattamento;
b) sia **autorizzata dal diritto dell'Unione o dello Stato membro** cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;
c) si basi sul **consenso esplicito** dell'interessato.

3. Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.

4. Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9 (vedi 3.3.1.6. Art.9: Trattamento di categorie particolari di dati personali), paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) (*n.d.r. l'interessato ha prestato il proprio consenso esplicito*) o g) (*n.d.r. trattamento necessario per motivi di interesse pubblico*), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

3.4.1.10. Art.12: Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato

Articolo 12 del Regolamento

1. Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le **informazioni** di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 (*n.d.r. diritto di accesso, diritto di rettifica, diritto di cancellazione, diritto di limitazione del trattamento, obbligo di notifica, diritto alla portabilità, diritto di opposizione, processo decisionale automatizzato*) e all'articolo 34 (vedi 3.9.1.2. Art.34: Comunicazione di una violazione dei dati personali all'interessato) relative al trattamento in f**orma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro**, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono **fornite per iscritto** o con altri mezzi, anche, se del caso, con **mezzi elettronici**. **Se richiesto dall'interessato, le**

informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

2. Il titolare del trattamento agevola l'esercizio dei diritti dell'interessato ai sensi degli articoli da 15 a 22 (*n.d.r. diritto di accesso, diritto di rettifica, diritto di cancellazione, diritto di limitazione del trattamento, obbligo di notifica, diritto alla portabilità, diritto di opposizione, processo decisionale automatizzato*). *Omissis*.

3. Il titolare del trattamento fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta ai sensi degli articoli da 15 a 22 (*n.d.r. diritto di accesso, diritto di rettifica, diritto di cancellazione, diritto di limitazione del trattamento, obbligo di notifica, diritto alla portabilità, diritto di opposizione, processo decisionale automatizzato*) senza ingiustificato ritardo e, comunque, al più tardi **entro un mese dal ricevimento della richiesta stessa**. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Il titolare del trattamento informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta. Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato.

4. Se non ottempera alla richiesta dell'interessato, il titolare del trattamento informa l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale.

5. Le informazioni fornite ai sensi degli articoli 13 e 14 ed eventuali comunicazioni e azioni intraprese ai sensi degli articoli da 15 a 22 (*n.d.r. diritto di accesso, diritto di rettifica, diritto di cancellazione, diritto di limitazione del trattamento, obbligo di notifica, diritto alla portabilità, diritto di opposizione, processo decisionale automatizzato*) e dell'articolo 34 (vedi 3.9.1.2. Art.34: Comunicazione di una violazione dei dati personali all'interessato) sono **gratuite**. Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento può:

a) addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta; oppure
b) rifiutare di soddisfare la richiesta.

Incombe al titolare del trattamento l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

6. *Omissis*.

7. Le informazioni da fornire agli interessati a norma degli articoli 13 e 14 possono essere fornite in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone sono leggibili da dispositivo automatico.

8. *Omissis*.

3.4.1.11. Art. 2-terdecies del Decreto 101/2018: Diritti riguardanti le persone decedute

Articolo 2-terdecies del Decreto 101/2018

1. I diritti di cui agli articoli da 15 a 22 del Regolamento riferiti ai dati personali concernenti **persone decedute** possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualita' di suo mandatario, o per ragioni familiari meritevoli di protezione.

2. L'esercizio dei diritti di cui al comma 1 non e' ammesso nei casi previsti dalla legge o quando, limitatamente all'offerta diretta di servizi della societa' dell'informazione, l'interessato lo ha espressamente vietato con dichiarazione scritta presentata al titolare del trattamento o a quest'ultimo comunicata.

3. La volonta' dell'interessato di vietare l'esercizio dei diritti di cui al comma 1 deve risultare in modo non equivoco e deve essere specifica, libera e informata; il divieto puo' riguardare l'esercizio soltanto di alcuni dei diritti di cui al predetto comma.

4. L'interessato ha in ogni momento il diritto di revocare o modificare il divieto di cui ai commi 2 e 3.

5. In ogni caso, il divieto non puo' produrre effetti pregiudizievoli per l'esercizio da parte dei terzi dei diritti patrimoniali che derivano dalla morte dell'interessato nonche' del diritto di difendere in giudizio i propri interessi.

3.4.2. Interpretazioni

3.4.2.1. Informativa agli interessati

In base al considerando 60, i principi di trattamento corretto e trasparente implicano che l'interessato sia informato dell'esistenza del trattamento e delle sue finalità. **Il titolare del trattamento dovrebbe fornire all'interessato eventuali ulteriori informazioni necessarie ad assicurare un trattamento corretto e trasparente**, prendendo in considerazione le circostanze e del contesto specifici in cui i dati personali sono trattati. Inoltre l'interessato dovrebbe essere informato dell'esistenza di una profilazione e delle conseguenze della stessa. In caso di dati personali raccolti direttamente presso l'interessato, questi dovrebbe inoltre essere informato dell'eventuale obbligo di fornire i dati personali e delle conseguenze in cui incorre se si rifiuta di fornirli.

Le informazioni fornite all'interessato relative al trattamento dei suoi dati personali sono comunemente definite ***informativa sul trattamento dei dati personali***.

Riassumendo il contenuto della informativa all'interessato dovrebbe essere conforme al presente schema:

Condizioni di presenza della sezione	***Sezione***	***Descrizione sezione***
	Dati del titolare del trattamento	identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
Se designato il responsabile della protezione dei dati	Dati del responsabile della protezione dei dati	dati di contatto del responsabile della protezione dei dati
	Finalità del trattamento	le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica[1] del trattamento
Se i dati non sono raccolti presso l'interessato	categorie di dati personali	categorie di dati personali trattati
Se il trattamento è necessario per il perseguimento del legittimo interesse	legittimi interessi	i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
Se i dati sono comunicati a terzi	destinatari	destinatario le categorie di destinatari dei dati personali
Se il titolare ha intenzione di trasferire i dati personale a un paese terzo o ad un'organizzazione internazionale	Trasferimento dei dati a paese extra-europeo o organizzazione internazionale	ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili
	Periodo di conservazione	periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo
	Diritti dell'interessato	l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati; c) qualora il trattamento sia basato sul consenso, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca; d) il diritto di proporre reclamo a un'autorità di controllo;

[1] Base giuridica

Se i dati sono raccolti presso l'interessato e se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto	Obbligo legale o contrattuale	l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati
Se i dati non sono raccolti presso l'interessato	Fonte di origine dei dati	la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;
Se esiste un processo decisionale automatizzato	Esistenza di un processo decisionale automatizzato (profilazione)	l'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.

Il considerando 58 recita che il principio della trasparenza impone che le informazioni destinate al pubblico o all'interessato siano **concise, facilmente accessibili e di facile comprensione e che sia usato un linguaggio semplice** e chiaro, oltre che, se del caso, una visualizzazione. Tali informazioni potrebbero essere fornite in formato elettronico, ad esempio, se destinate al pubblico, attraverso un sito web. Ciò è particolarmente utile in situazioni in cui la molteplicità degli operatori coinvolti e la complessità tecnologica dell'operazione fanno sì che sia difficile per l'interessato comprendere se, da chi e per quali finalità sono raccolti dati personali che lo riguardano, quali la pubblicità online. Dato che i minori meritano una protezione specifica, quando il trattamento dati li riguarda, qualsiasi informazione e comunicazione dovrebbe utilizzare un linguaggio semplice e chiaro che un minore possa capire facilmente.

Infine per il considerando 61 l'interessato dovrebbe **ricevere le informazioni relative al trattamento di dati personali che lo riguardano al momento della raccolta** presso l'interessato o, se i dati sono ottenuti da altra fonte, entro un termine ragionevole, in funzione delle circostanze del caso. Se i dati personali possono essere legittimamente comunicati a un altro destinatario, l'interessato dovrebbe esserne informato nel momento in cui il destinatario riceve la prima comunicazione dei dati personali. Il titolare del trattamento, qualora intenda trattare i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, dovrebbe fornire all'interessato, prima di tale ulteriore trattamento, informazioni in merito a tale finalità diversa e altre informazioni necessarie. Qualora non sia possibile comunicare all'interessato l'origine dei dati personali, perché sono state utilizzate varie fonti, dovrebbe essere fornita un'informazione di carattere generale.

In caso di attività professionale, l'informativa deve essere fornita nella maggior parte dei casi alle seguenti categorie di interessati

- **clienti e committenti**: normalmente un professionista tratta dati personali di persone fisiche che rappresentano clienti/committenti, ad esempio nome, cognome, telefono, e-mail, recapiti postali, ecc.;
- **fornitori**: quando questi sono persone fisiche, i dati relativi a persone giuridiche o società non sono da considerarsi come dati personali;

- **dipendenti e collaboratori**: i collaboratori possono ricadere nella categoria dei fornitori persone fisiche se prestano principalmente consulenze saltuarie, non continuative;
- **soggetti terzi**: come ad esempio direttori dei lavori, progettisti di altre discipline, rappresentanti di Imprese appaltatrici, partner, ecc..

L'informativa ha di solito forma scritta e può essere distribuita agli interessati tramite e-mail, può essere pubblicata sul sito internet professionale, può essere allegata al contratto di fornitura, o consegnata a mano come documento cartaceo a se stante.

Sorge in molti casi la problematica di come dimostrare di aver fornito l'informativa all'interessato. Anche in questo caso il Regolamento non dà indicazioni precise ma lascia l'onere della prova al titolare.

Può essere utile in tal senso conservare le e-mail inviate agli interessati, o in caso di informativa cartacea aggiungere una dicitura "ho letto e compreso" da corredare con la firma dell'interessato.

3.4.2.2. Altri diritti dell'interessato

Ulteriori approfondimenti sono disponibili nel paragrafo 8.4. I diritti dell'interessato.

Il Garante mette a disposizione un modello per consentire all'interessato di esercitare i propri diritti, disponibile al seguente link

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9038275

3.5. Ruoli, responsabilità, compiti

3.5.1. Cosa dice la normativa

3.5.1.1. Art.24: Responsabilità del titolare del trattamento

Articolo 24 del Regolamento

1. Tenuto 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, il **titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento**. Dette misure sono riesaminate e aggiornate qualora necessario.

2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.

3. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 (*n.d.r. codici di condotta e certificazione*) può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

3.5.1.2. Art.26: Contitolari del trattamento

Articolo 26 del Regolamento

1. Allorché **due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento**. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14 (vedi 3.4.1.1. Art.13,14 del Regolamento e Art.111-bis del Decreto 101/2018: Informazioni all'interessato relative al trattamento dei dati personali), a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati.

2. L'accordo di cui al paragrafo 1 riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

3. Indipendentemente dalle disposizioni dell'accordo di cui al paragrafo 1, l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun titolare del trattamento.

3.5.1.3. Art.28,29: Responsabile del trattamento

Articoli 28 del Regolamento: Responsabile del trattamento

1. Qualora un **trattamento debba essere effettuato per conto del titolare del trattamento**, quest'ultimo ricorre unicamente a **responsabili del trattamento** che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

2. **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 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.

3. **I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico** a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il **responsabile del trattamento**:

a) **tratti i dati personali soltanto su istruzione documentata del titolare del trattamento**, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento

informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

b) **garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza** o abbiano un adeguato obbligo legale di riservatezza;
c) **adotti tutte le misure richieste** ai sensi dell'articolo 32 (vedi 3.8.1.1. Art.32: Misure di sicurezza tecniche e organizzative);
d) **rispetti le condizioni** di cui ai paragrafi 2 e 4 **per ricorrere a un altro responsabile del trattamento**;
e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;
f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 (*n.d.r. sicurezza dei dati personali e valutazione d'impatto*) , tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e
h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

Con riguardo alla lettera h) del primo comma, il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

4. Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, **su tale altro responsabile del trattamento sono imposti**, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, **gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento** di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

5. L'adesione da parte del responsabile del trattamento a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 *(n.d.r. codici di condotta e certificazione*) può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai paragrafi 1 e 4 del presente articolo.

6. *Omissis*

7. *Omissis*

8. *Omissis*

9. Il **contratto o altro atto giuridico** di cui ai paragrafi 3 e 4 è **stipulato in forma scritta, anche in formato elettronico**.

10. Fatti salvi gli articoli 82 (vedi 3.11.1.3. Art.82: Diritto al risarcimento e responsabilità), 83 (vedi 3.11.1.4. Art.83: Condizioni generali per infliggere sanzioni amministrative pecuniarie) e 84 (vedi 3.11.1.5. Art. 84: Sanzioni), **se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento** in questione.

Articoli 29 del Regolamento: Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento

Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

3.5.1.4. Art.37,38,39: Responsabile della protezione dei dati (Data Protection Officer)

Articolo 37 del Regolamento: Designazione del responsabile della protezione dei dati

1. Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogni qualvolta:

a) il trattamento è effettuato da un'**autorità pubblica o da un organismo pubblico**, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il **monitoraggio regolare e sistematico degli interessati su larga scala**; oppure
c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel **trattamento, su larga scala, di categorie particolari di dati personali** di cui all'articolo 9 (vedi 3.3.1.6. Art.9: Trattamento di categorie particolari di dati personali) o di **dati relativi a condanne penali e a reati** di cui all'articolo 10 (vedi 3.3.1.7. Art.10: Trattamento di dati personali relativi a condanne penali e reati).

2. *Omissis*

3. *Omissis*

4. *Omissis*

5. 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.

6. Il responsabile della protezione dei dati **può essere un dipendente** del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un **contratto di servizi**.

7. Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo.

Articolo 38 del Regolamento: Posizione del responsabile della protezione dei dati

1. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

2. Il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.

3. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.

4 Gli interessati possono 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.

5. Il responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri.

6. Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi.

Articolo 39 del Regolamento: Compiti del responsabile della protezione dei dati

1. 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 (vedi 3.8.1.2. Art.35,36: Valutazione d'impatto e consultazione preventiva);
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 (vedi 3.8.1.2. Art.35,36: Valutazione d'impatto e consultazione preventiva), ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

2. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

3.5.1.5. Art. 31: Cooperazione con l'autorità di controllo

Articolo 31 del Regolamento

Il titolare del trattamento, il responsabile del trattamento e, ove applicabile, il loro rappresentante cooperano, su richiesta, con l'autorità di controllo nell'esecuzione dei suoi compiti.

3.5.1.6. Art. 2-quaterdecies del Decreto 101/2018: Attribuzione di funzioni e compiti a soggetti designati

Articolo 2-quaterdecies del Decreto 101/2018

1. **Il titolare o il responsabile del trattamento possono prevedere**, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici **compiti e funzioni** connessi al trattamento di dati personali siano **attribuiti a persone fisiche, espressamente designate**, che operano sotto la loro autorità.

2. Il titolare o il responsabile del trattamento individuano le modalità più opportune per **autorizzare al trattamento** dei dati personali le persone che operano sotto la propria autorità diretta.

3.5.2. Interpretazioni

3.5.2.1. Responsabilità del titolare del trattamento

Il *Titolare del trattamento* è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

Il titolare è perciò colui a cui gli interessati hanno affidato dei dati personali e diventa colui che è responsabile di come questi verranno trattati, sia dalla sua organizzazione che da collaboratori esterni (sia che si tratti di un libero professionista, di uno studio professionale o di una società).

Il principio di responsabilizzazione (vedi paragrafi 3.3.1.1. Art.5:Principi applicabili al trattamento di dati personali e 8.3. Principio di responsabilizzazione o "accountability") determina che non ci sono vie d'uscite legali per il titolare se i dati personali non vengano trattati in conformità con la normativa; se il titolare delega la decisione delle misure da adottare o una gestione ad un fornitore e questi lo fa in modo non corretto la responsabilità è sempre in solido e ricade in prima

battuta sul titolare che ha la responsabilità nei confronti degli interessati delle azioni dei collaboratori che sceglie e cui affida i dati.

Il titolare inoltre deve valutare in prima persona il grado di rischio su come gestisce o fa gestire i dati sia dal punto di vista sia tecnico che organizzativo e se ne deve fare responsabile a priori dimostrando lui stesso che a suo avviso ha adottato le misure necessarie e non aspettando che qualcuno dimostri il contrario.

3.5.2.2. Contitolare del trattamento

Potenzialmente la **titolarità dei dati personali dell'interessato può essere condivisa** se questo viene reso trasparente all'interessato stesso che accetta tale condizione.

Ad esempio quando si fanno degli eventi di marketing in partnership congiunta e si decide che gli inviti o le iscrizioni a tali eventi possono diventare dati trattati poi dai vari partner per determinate finalità.

A differenza della nomina a responsabile dei trattamenti che rappresenta un delegato del titolare per una sua finalità, il contitolare determina insieme al titolare sia le finalità che i mezzi di gestione del trattamento. La responsabilità nei confronti dell'interessato è congiunta a meno che non sia chiaramente confinata tra i due contitolari da un accordo scritto di cui l'interessato è a conoscenza per poter esercitare correttamente i propri i diritti nei confronti dell'uno o dell'altro.

3.5.2.3. Responsabile del trattamento

Quando un **titolare affida ad un altro soggetto (generalmente un fornitore) un'attività di trattamento da svolgere "per proprio conto"**, quest'ultimo deve essere designato ***Responsabile del trattamento***.

È una figura prettamente esterna alla struttura del titolare, da non confondere con gli Incaricati del trattamento, la cui nomina era obbligatoria per il Codice Privacy Italiano.

I **responsabili del trattamento devono presentare garanzie sufficienti** per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento garantisca la tutela dei diritti dell'interessato: è responsabilità del titolare verificare tali requisiti.

I **trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico**, che vincoli il responsabile del trattamento al titolare del trattamento e che

a) stipuli la materia disciplinata e la **durata del trattamento,**
b) stipuli **la natura e la finalità del trattamento,**
c) stipuli **il tipo di dati personali e le categorie di interessati,**
d) stipuli **gli obblighi e i diritti del titolare del trattamento**,
e) garantisca che le persone autorizzate al trattamento dei dati personali si siano **impegnate alla riservatezza** o abbiano un adeguato obbligo legale di riservatezza,
f) garantisca l'assistenza al titolare del trattamento al fine di soddisfare l'obbligo di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
g) garantisca che il responsabile adotti tutte le misure di sicurezza descritte nel paragrafo 3.8.1.1. Art.32: Misure di sicurezza tecniche e organizzative e assista il titolare del trattamento nel garantire il rispetto degli obblighi di sicurezza del trattamento;

h) garantisca che il responsabile, su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti;
i) garantisca che il responsabile metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui sopra e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato;
j) garantisca che il responsabile rispetti le condizioni di cui sopra per ricorrere a un altro responsabile del trattamento;

Il titolare deve inoltre fornire al responsabile **istruzione documentata del titolare sulle modalità di trattamento, viceversa il responsabile deve** trattare i dati personali soltanto su **istruzione documentata del titolare del trattamento.**

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 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.

Quando un **responsabile del trattamento ricorre a un altro responsabile** del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, **su tale altro responsabile del trattamento sono imposti**, mediante un contratto o un altro atto giuridico, **gli stessi obblighi** in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, **il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi** dell'altro responsabile.

Il **contratto o altro atto giuridico tra titolare e responsabile è stipulato in forma scritta, anche in formato elettronico**.

Escludendo i fini sanzionatori, se un responsabile del trattamento determina le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione.

3.5.2.4. Soggetti autorizzati al trattamento

Il ***soggetto autorizzato al trattamento dei dati personali* è la persona fisica che effettua materialmente le operazioni di trattamento sui dati personali sotto l'autorità diretta del titolare o del responsabile**.

Il Garante nella *Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali - TITOLARE, RESPONSABILE, INCARICATO DEL TRATTAMENTO* precisa che, pur non prevedendo espressamente la figura dell' "incaricato" del trattamento (ex Articolo 30 del Codice Privacy), il Regolamento non ne esclude la presenza e fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile".

Tanto che l'articolo 2-quaterdecies del Decreto 101/2018 recita che "il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio

assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità" e che "il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta".

Pertanto nè Il Regolamento nè il Decreto 101/2018 prevedono l'obbligo di nomina o designazione espressa dei soggetti autorizzati al trattamento.

Tuttavia gli articoli 29 (vedi 3.5.1.3. Art.28,29: Responsabile del trattamento) e 32 (vedi 3.8.1.1. Art.32: Misure di sicurezza tecniche e organizzative) del Regolamento, impongono che **chiunque agisca sotto l'autorità del titolare o del responsabile del trattamento**, che abbia accesso a dati personali non può trattare tali dati se non è **istruito** in tal senso dal titolare del trattamento (vedi 7.2. (In)formarsi e (in)formare).

Inoltre l'articolo 28 del Regolamento (vedi 3.5.1.3. Art.28,29: Responsabile del trattamento) richiede che il responsabile del trattamento garantisca che le persone autorizzate al trattamento dei dati personali si siano **impegnate alla riservatezza** o abbiano un adeguato obbligo legale di riservatezza: tale buona pratica è applicabile anche da parte del titolare ai soggetto autorizzati alle sue dipendenze.

Pertanto risulta

- **consigliato, sia per il titolare che per il responsabile, designare i soggetti autorizzati al trattamento dei dati personali** che operano sotto la sua diretta autorità,
- **consigliato, al titolare, di garantire che i soggetti autorizzati** che operano sotto la sua diretta autorità siano **impegnati alla riservatezza**,
- **richiesto** dall' articolo 28 del Regolamento, **al responsabile, di garantire al titolare che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza** o abbiano un adeguato obbligo legale di riservatezza;
- **richiesto** dagli articoli 29 e 32, sia al responsabile sia al titolare, che o**gni soggetto autorizzato al trattamento sotto la sua autorità non tratti i dati personali se non è istruito** in tal senso dal titolare del trattamento.

L'eventuale atto di designazione a soggetto incaricato al trattamento di dati personali non necessita di firma per accettazione, anche se è utile un' attestazione di presa visione, in particolare se l'atto è corredato delle istruzioni sul trattamento dei dati personali, a dimostrazione dell'impartizione delle istruzioni stesse.

3.5.2.5. Responsabile della protezione dei dati (Data Protection Officer)

Sull'obbligatorietà della designazione del responsabile della protezione dei dati personali per liberi professionisti e piccoli studi professionali si sono espressi sia il Gruppo Art.29 che il Garante stesso.

Le *Linee guida sui responsabili della protezione dei dati (WP 243 rev. 01)* del Gruppo Art. 29 annoverano tra i trattamenti che si possono considerare non su larga scala, e che quindi non renderebbero di per sé obbligatoria la designazione di un responsabile della protezione dei dati:

- trattamento di dati relativi a pazienti svolto da un singolo professionista sanitario;
- trattamento di dati personali relativi a condanne penali e reati svolto da un singolo avvocato.

Analogamente le *Nuove Faq sul Responsabile della Protezione dei Dati (RPD) in ambito privato* del Garante della Privacy come esempio di trattamenti per i quali la designazione del responsabile del trattamento non è obbligatoria

- trattamenti effettuati da liberi professionisti operanti in forma individuale;
- agenti, rappresentanti e mediatori operanti non su larga scala;
- imprese individuali o familiari;
- piccole e medie imprese, con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti.

In base a tali considerazioni, **per i liberi professionisti operanti in forma individuale e per gli studi professionali si può ritenere non obbligatoria la designazione del responsabile della protezione dei dati**, a meno che le attività principali svolte non richiedano il monitoraggio regolare e sistematico degli interessati su larga scala e non consistano nel trattamento, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali e a reati.

3.6. Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali

3.6.1. Cosa dice la normativa

3.6.1.1. Art.44: Principio generale per il trasferimento

Articolo 44 del Regolamento

Qualunque **trasferimento di dati personali** oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento **verso un paese terzo o un'organizzazione internazionale**, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, ha luogo soltanto **se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni** seguenti.

3.6.1.2. Art.45: Trasferimento sulla base di una decisione di adeguatezza

Articolo 45 del Regolamento

1. Il **trasferimento di dati personali verso un paese terzo** o un'organizzazione internazionale **è ammesso se la Commissione ha deciso che il paese** terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione **garantiscono un livello di protezione adeguato**. In tal caso il trasferimento non necessita di autorizzazioni specifiche.

2. *Omissis*

3. *Omissis*

4. *Omissis*

5. *Omissis*

6. *Omissis*

7. *Omissis*

8. La Commissione pubblica nella Gazzetta ufficiale dell'Unione europea e sul suo sito web l'elenco dei paesi terzi, dei territori e settori specifici all'interno di un paese terzo, e delle organizzazioni internazionali per i quali ha deciso che è o non è più garantito un livello di protezione adeguato.

9. *Omissis*

3.6.1.3. Art.46: Trasferimento soggetto a garanzie adeguate

Articolo 46 del Regolamento

1. In mancanza di una decisione ai sensi dell'articolo 45 (vedi 3.6.1.2. Art.45: Trasferimento sulla base di una decisione di adeguatezza), paragrafo 3, il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi.

2. Possono **costituire garanzie adeguate** di cui al paragrafo 1 senza necessitare di autorizzazioni specifiche da parte di un'autorità di controllo:

a) uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici;
b) le **norme vincolanti d'impresa** in conformità dell'articolo 47;
c) le clausole tipo di protezione dei dati adottate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2;
d) le clausole tipo di protezione dei dati adottate da un'autorità di controllo e approvate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2;
e) un codice di condotta approvato a norma dell'articolo 40,unitamente all'impegno vincolante ed esecutivo da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati; o
f) un meccanismo di certificazione approvato a norma dell'articolo 42, unitamente all'impegno vincolante ed esigibile da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati.

3. Fatta salva l'autorizzazione dell'autorità di controllo competente, possono altresì costituire in particolare garanzie adeguate di cui al paragrafo 1:

a) le clausole contrattuali tra il titolare del trattamento o il responsabile del trattamento e il titolare del trattamento, il responsabile del trattamento o il destinatario dei dati personali nel paese terzo o nell'organizzazione internazionale; o
b) le disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli interessati.

4. *Omissis*

5. *Omissis*

3.6.1.4. Art.47: Norme vincolanti d'impresa

Articolo 47 del Regolamento

1. L'autorità di controllo competente approva le norme vincolanti d'impresa in conformità del meccanismo di coerenza di cui all'articolo 63, a condizione che queste:

a) siano giuridicamente vincolanti e si applichino a tutti i membri interessati del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune, compresi i loro dipendenti;
b) conferiscano espressamente agli interessati diritti azionabili in relazione al trattamento dei loro dati personali; e
c) soddisfino i requisiti di cui al paragrafo 2.

2. Le norme vincolanti d'impresa di cui al paragrafo 1 specificano almeno:

a) la struttura e le coordinate di contatto del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e di ciascuno dei suoi membri;
b) i trasferimenti o il complesso di trasferimenti di dati, in particolare le categorie di dati personali, il tipo di trattamento e relative finalità, il tipo di interessati cui si riferiscono i dati e l'identificazione del paese terzo o dei paesi terzi in questione;
c) la loro natura giuridicamente vincolante, a livello sia interno che esterno;
d) l'applicazione dei principi generali di protezione dei dati, in particolare in relazione alla limitazione della finalità, alla minimizzazione dei dati, alla limitazione del periodo di conservazione, alla qualità dei dati, alla protezione fin dalla progettazione e alla protezione per impostazione predefinita, alla base giuridica del trattamento e al trattamento di categorie particolari di dati personali, le misure a garanzia della sicurezza dei dati e i requisiti per i trasferimenti successivi ad organismi che non sono vincolati dalle norme vincolanti d'impresa;
e) i diritti dell'interessato in relazione al trattamento e i mezzi per esercitarli, compresi il diritto di non essere sottoposto a decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione ai sensi dell'articolo 22, il diritto di proporre reclamo all'autorità di controllo competente e di ricorrere alle autorità giurisdizionali competenti degli Stati membri conformemente all'articolo 79, e il diritto di ottenere riparazione e, se del caso, il risarcimento per violazione delle norme vincolanti d'impresa;
f) il fatto che il titolare del trattamento o il responsabile del trattamento stabilito nel territorio di uno Stato membro si assume la responsabilità per qualunque violazione delle norme vincolanti d'impresa commesse da un membro interessato non stabilito nell'Unione; il titolare del trattamento o il responsabile del trattamento può essere esonerato in tutto o in

parte da tale responsabilità solo se dimostra che l'evento dannoso non è imputabile al membro in questione;

g) le modalità in base alle quali sono fornite all'interessato le informazioni sulle norme vincolanti d'impresa, in particolare sulle disposizioni di cui alle lettere d), e) e f), in aggiunta alle informazioni di cui agli articoli 13 e 14 (vedi 3.4.1.1. Art.13,14 del Regolamento e Art.111-bis del Decreto 101/2018: Informazioni all'interessato relative al trattamento dei dati personali);

h) omissis

i) omissis

j) omissis

k) omissis

l) omissis

m) omissis

n) l'appropriata formazione in materia di protezione dei dati al personale che ha accesso permanente o regolare ai dati personali.

3. *Omissis*

3.6.1.5. Art.49: Deroghe in specifiche situazioni

Articolo 49 del Regolamento

1. In mancanza di una decisione di adeguatezza ai sensi dell'articolo 45 (vedi 3.6.1.2. Art.45: Trasferimento sulla base di una decisione di adeguatezza), paragrafo 3, o di garanzie adeguate ai sensi dell'articolo 46 (vedi 3.6.1.3. Art.46: Trasferimento soggetto a garanzie adeguate), comprese le norme vincolanti d'impresa, è ammesso il trasferimento o un complesso di trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale soltanto se si verifica una delle seguenti condizioni:

a) l'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti per l'interessato, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate;

b) il trasferimento sia necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato;

c) il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato;

d) il trasferimento sia necessario per importanti motivi di interesse pubblico;

e) il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;

f) il trasferimento sia necessario per tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

g) *omissis*.

Se non è possibile basare il trasferimento su una disposizione dell'articolo 45 (vedi 3.6.1.2. Art.45: Trasferimento sulla base di una decisione di adeguatezza) o 46 (vedi 3.6.1.3. Art.46: Trasferimento soggetto a garanzie adeguate), comprese le disposizioni sulle

norme vincolanti d'impresa, e nessuna delle deroghe in specifiche situazioni a norma del primo comma del presente paragrafo è applicabile, il trasferimento verso un paese terzo o un'organizzazione internazionale sia ammesso soltanto se non è ripetitivo, riguarda un numero limitato di interessati, è necessario per il perseguimento degli interessi legittimi cogenti del titolare del trattamento, su cui non prevalgano gli interessi o i diritti e le libertà dell'interessato, e qualora il titolare e del trattamento abbia valutato tutte le circostanze relative al trasferimento e sulla base di tale valutazione abbia fornito garanzie adeguate relativamente alla protezione dei dati personali. Il titolare del trattamento informa del trasferimento l'autorità di controllo. In aggiunta alla fornitura di informazioni di cui agli articoli 13 e 14 (vedi 3.4.1.1. Art.13,14 del Regolamento e Art.111-bis del Decreto 101/2018: Informazioni all'interessato relative al trattamento dei dati personali), il titolare del trattamento informa l'interessato del trasferimento e degli interessi legittimi cogenti perseguiti.

2. *Omissis*

3. *Omissis*

4. *Omissis*

5. *Omissis*

6. Il titolare del trattamento o il responsabile del trattamento attesta nel registro di cui all'articolo 30 (vedi 3.7. Art.30: Registri delle attività di trattamento) la valutazione e le garanzie adeguate di cui al paragrafo 1, secondo comma, del presente articolo.

3.6.2. Interpretazioni

Il capo V tratta nei sei articoli che lo compongono del trasferimento dei dati dell'interessato da parte del titolare o del responsabile del trattamento dei dati garantendo che "il livello di protezione delle persone fisiche garantito dal presente regolamento non sia pregiudicato" (art. 44).

Se il paese terzo o l'organizzazione internazionale presso i quali si trasferiscono i dati personali garantiscono un livello di protezione adeguato, deciso dalla Commissione, il trasferimento non necessita di autorizzazione specifica. **La Commissione pubblica nella Gazzetta ufficiale dell'Unione Europea e sul suo sito web l'elenco dei paesi terzi e delle organizzazioni internazionali per i quali ha deciso che è o non è più garantito un livello di protezione adeguato**, si segnala in particolare il seguente link : https://www.garanteprivacy.it/home/provvedimenti-normativa/normativa/normativa-comunitaria-e-intenazionale/trasferimento-dei-dati-verso-paesi-terzi.

In mancanza di una decisione di adeguatezza, il titolare o il responsabile "può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se ha fornito **garanzie adeguate** e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi" tra cui:

- norme vincolanti d'impresa (articolo 47 del Regolamento);
- codice di condotta approvato (*Articolo 40* del Regolamento) assieme all'impegno vincolante ed esecutivo di applicare le garanzie adeguate;
- meccanismo di certificazione (*Articolo 42* del Regolamento);
- clausole contrattuali tra i titolari del trattamento;

- disposizioni da inserire in accordi amministrativi che comprendono diritti effettivi per gli interessati.

3.7. Art.30: Registri delle attività di trattamento

3.7.1. Cosa dice la normativa

Articolo 30 del Regolamento

1. Ogni **titolare del trattamento** e, ove applicabile, il suo rappresentante tengono un **registro delle attività di trattamento** svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

a) **il nome e i dati di contatto del titolare del trattamento** e, ove applicabile, del **contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati**;
b) le **finalità del trattamento**;
c) una descrizione delle **categorie di interessati** e delle **categorie di dati personali**;
d) le **categorie di destinatari** a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
e) ove applicabile, i **trasferimenti di dati personali verso un paese terzo** o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
f) ove possibile, i **termini ultimi previsti per la cancellazione** delle diverse categorie di dati;
g) ove possibile, una descrizione generale delle **misure di sicurezza tecniche e organizzative** di cui all'articolo 32 (vedi 3.8.1.1. Art.32: Misure di sicurezza tecniche e organizzative), paragrafo 1.

2. Ogni **responsabile del trattamento** e, ove applicabile, il suo rappresentante tengono un **registro di tutte le categorie di attività relative al trattamento** svolte per conto di un titolare del trattamento, contenente:

a) **il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati**;
b) le **categorie dei trattamenti effettuati** per conto di ogni titolare del trattamento;
c) ove applicabile, i **trasferimenti di dati personali verso un paese terzo** o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
d) ove possibile, una descrizione generale delle **misure di sicurezza tecniche e organizzative** di cui all'articolo 32 (vedi 3.8.1.1. Art.32: Misure di sicurezza tecniche e organizzative), paragrafo 1.

3. I registri di cui ai paragrafi 1 e 2 sono tenuti in **forma scritta**, anche in **formato elettronico**.

4. Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.

5. Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9 (vedi 3.3.1.6. Art.9: Trattamento di categorie particolari di dati personali), paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10 (vedi 3.3.1.7. Art.10: Trattamento di dati personali relativi a condanne penali e reati).

3.7.2. Interpretazioni

In base alle *FAQ sul registro delle attività di trattamento* di cui il comunicato stampa dell' 08/10/2018 del Garante, si specifica quanto segue.

E' un documento contenente le principali informazioni (specificatamente individuate dall' *Articolo 30* del Regolamento - vedi 3.7. Art.30: Registri delle attività di trattamento) relative alle operazioni di trattamento svolte dal titolare e, se nominato, dal responsabile del trattamento.

Il registro delle attività di trattamento costituisce uno dei principali elementi di accountability del titolare, in quanto strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, indispensabile per ogni attività di valutazione o analisi del rischio e dunque preliminare rispetto a tali attività.

Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.
I titolari e i responsabili del trattamento che, in ambito privato, sono tenuti a redigere il Registro delle attività di trattamento sono così individuabili:

- imprese o organizzazioni con almeno 250 dipendenti;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti che possano presentare un rischio – anche non elevato – per i diritti e le libertà dell'interessato;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti non occasionali;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti delle categorie particolari di dati di cui all' articolo 9 del Regolamento (vedi 3.3.1.6. Art.9: Trattamento di categorie particolari di dati personali), o di dati personali relativi a condanne penali e a reati di cui all' articolo 10 del Regolamento (vedi 3.3.1.7. Art.10: Trattamento di dati personali relativi a condanne penali e reati).

Rientrano nella categoria delle "organizzazioni" di cui all'articolo 30 del Regolamento (vedi 3.7. Art.30: Registri delle attività di trattamento), anche le associazioni, fondazioni e i comitati.

Alla luce di quanto detto sopra, **sono tenuti all'obbligo di redazione del registro**, ad esempio:

- **esercizi commerciali, esercizi pubblici o artigiani con almeno un dipendente** (bar, ristoranti, officine, negozi, piccola distribuzione, ecc.) **e/o che trattino dati sanitari dei clienti** (es. parrucchieri, estetisti, ottici, odontotecnici, tatuatori ecc.);

- **liberi professionisti con almeno un dipendente e/o che trattino dati sanitari e/o dati relativi a condanne penali o reati** (es. commercialisti, notai, avvocati, osteopati, fisioterapisti, farmacisti, medici in generale);
- associazioni, fondazioni e comitati ove trattino "categorie particolari di dati" e/o dati relativi a condanne penali o reati (i.e. organizzazioni di tendenza; associazioni a tutela di soggetti c.d. "vulnerabili" quali ad esempio malati, persone con disabilità, ex detenuti ecc.; associazioni che perseguono finalità di prevenzione e contrasto delle discriminazioni di genere, razziali, basate sull'orientamento sessuale, politico o religioso ecc.; associazioni sportive con riferimento ai dati sanitari trattati; partiti e movimenti politici; sindacati; associazioni e movimenti a carattere religioso);
- **il condominio ove tratti "categorie particolari di dati"** (es. delibere per interventi volti al superamento e all'abbattimento delle barriere architettoniche ai sensi della L. n. 13/1989; richieste di risarcimento danni comprensive di spese mediche relativi a sinistri avvenuti all'interno dei locali condominiali).

Infine, si precisa che le imprese e organizzazioni con meno di 250 dipendenti obbligate alla tenuta del registro potranno comunque beneficiare di alcune misure di semplificazione, potendo circoscrivere l'obbligo di redazione del registro alle sole specifiche attività di trattamento sopra individuate (es. ove il trattamento delle categorie particolari di dati si riferisca a quelli inerenti un solo lavoratore dipendente, il registro potrà essere predisposto e mantenuto esclusivamente con riferimento a tale limitata tipologia di trattamento).

Al di fuori dei casi di tenuta obbligatoria del Registro, anche alla luce del considerando 82 del Regolamento, i**l Garante ne raccomanda la redazione a tutti i titolari e responsabili del trattamento**, in quanto strumento che, fornendo piena contezza del tipo di trattamenti svolti, contribuisce a meglio attuare, con modalità semplici e accessibili a tutti, il principio di accountability e, al contempo, ad agevolare in maniera dialogante e collaborativa l'attività di controllo del Garante stesso.

Il registro del titolare potrebbe essere a sommi capi organizzato in questo modo

Intestazione : (a) il **nome e i dati di contatto** del titolare del trattamento e, ove applicabile, del contitolare del trattamento e del responsabile della protezione dei dati (DPO)
Per ogni trattamento svolto come titolare descrizione del **trattamento** (b) **finalità** del trattamento (c) descrizione delle **categorie di interessati** e delle **categorie di dati personali** (d) **categorie di destinatari** a cui i dati personali sono stati o saranno comunicati, compresi responsabili, contitolari e titolari autonomi del trattamento (e) ove applicabile il **trasferimento** di dati personali **verso un paese terzo** (f) ove possibile i **termini ultimi** previsti per la **cancellazione** delle diverse categorie di dati (g) eventuale descrizione delle **misure di sicurezza** tecniche e organizzative pertinenti al trattamento
(g) Eventuale descrizione generale delle **misure di sicurezza** applicabili a tutti i trattamenti

Il registro del responsabile potrebbe essere a sommi capi organizzato in questo modo

Intestazione : (a) **nome e i dati di contatto** del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento e ove applicabile, del DPO
Per ogni trattamento svolto per conto di titolare (b) titolare/i per conto del/i quale/i si svolge il trattamento (se le attività sono svolte per più di un titolare) (b) descrizione del **trattamento** (c) ove applicabile il **trasferimento** di dati personali **verso un paese terzo** (d) eventuale descrizione delle **misure di sicurezza** tecniche e organizzative pertinenti al trattamento
(d) Eventuale descrizione generale delle **misure di sicurezza** applicabili a tutti i trattamenti

Il registro deve essere **sempre aggiornato** e disponibile.

Nel rispetto del principio di responsabilizzazione, può essere utile attribuire una **versione** ad ogni copia del registro e **mantenere lo storico** delle versioni precedenti per facilitare la gestione delle eventuali violazioni dei dati personali e l'attività ispettiva del Garante.

L'allegato 9.1. GDPR toolkit per i professionisti presenta un modello per la raccolta delle informazioni e la redazione dei registri delle attività di trattamento.

3.8. Protezione dei dati e valutazione del rischio

3.8.1. Cosa dice la normativa

3.8.1.1. Art.32: Misure di sicurezza tecniche e organizzative

Articolo 32 del Regolamento

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, **il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio**, che comprendono, tra le altre, se del caso:

a) la **pseudonimizzazione** e la **cifratura dei dati personali**;
b) la capacità di assicurare su base permanente la **riservatezza, l'integrità, la disponibilità e la resilienza** dei sistemi e dei servizi di trattamento;
c) la capacità di **ripristinare tempestivamente la disponibilità** e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, **verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative** al fine di garantire la sicurezza del trattamento.

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei **rischi** presentati dal trattamento che derivano in particolare dalla **distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata** o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.

4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

3.8.1.2. Art.35,36: Valutazione d'impatto e consultazione preventiva

Articolo 35 del Regolamento: Valutazione d'impatto sulla protezione dei dati

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. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.

3. La **valutazione d'impatto** sulla protezione dei dati di cui al paragrafo 1 **è richiesta** in particolare nei casi seguenti:

a) 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**;
b) il **trattamento, su larga scala, di categorie particolari di dati personali** di cui all'articolo 9 (vedi 3.3.1.6. Art.9: Trattamento di categorie particolari di dati personali), paragrafo 1, **o di dati relativi a condanne penali e a reati** di cui all'articolo 10 (vedi 3.3.1.7. Art.10: Trattamento di dati personali relativi a condanne penali e reati); o
c) la **sorveglianza sistematica su larga scala di una zona accessibile al pubblico**.

4. *Omissis*

5. *Omissis*

6. *Omissis*

7. La valutazione contiene almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e
d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

8. Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.

9. Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.

10. *Omissis*

11. Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.

Articolo 36 del Regolamento: Consultazione preventiva

1. Il titolare del trattamento, **prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto** sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento **presenterebbe un rischio elevato in assenza di misure** adottate dal titolare del trattamento per attenuare il rischio.

2. Se ritiene che il trattamento previsto di cui al paragrafo 1 violi il presente regolamento, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, l'autorità di controllo fornisce, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto al titolare del trattamento e, ove applicabile, al responsabile del trattamento e può avvalersi dei poteri di cui all'articolo 58 (vedi 3.10.1.3. Art.58: Poteri dell'autorità di controllo). Tale periodo può essere prorogato di sei settimane, tenendo conto della complessità del trattamento previsto. L'autorità di controllo informa il titolare del trattamento e, ove applicabile, il responsabile del trattamento di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione. La decorrenza dei termini può essere sospesa fino all'ottenimento da parte dell'autorità di controllo delle informazioni richieste ai fini della consultazione.

3. Al momento di consultare l'autorità di controllo ai sensi del paragrafo 1, il titolare del trattamento comunica all'autorità di controllo:

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 responsabile della protezione dei dati;
e) la valutazione d'impatto sulla protezione dei dati di cui all'articolo 35; e
f) ogni altra informazione richiesta dall'autorità di controllo.

4. *Omissis*

5. *Omissis*

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

Articolo 25 del Regolamento

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, **sia al**

momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento **mette in atto misure tecniche e organizzative adeguate**, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

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

3. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo.

3.8.2. Interpretazioni

Come esposto nel considerando 78, la tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del Regolamento.

Al fine di poter dimostrare la conformità con il presente regolamento, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default. Tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, pseudonimizzare i dati personali il più presto possibile, offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali, consentire all'interessato di controllare il trattamento dei dati e consentire al titolare del trattamento di creare e migliorare caratteristiche di sicurezza.

In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati.

L'adeguatezza delle misure di sicurezza in relazione al rischio per la libertà e i diritti delle persone fisiche può essere valutata in base quanto esposto nel paragrafo 4. VALUTAZIONE E GESTIONE DEI RISCHI PER I DIRITTI E LE LIBERTÀ DELLE PERSONE FISICHE.

Il titolare o il responsabile ha l'obbligo anche di identificare i trattamenti, anche in funzione della valutazione del rischio di cui sopra, che necessitino di una valutazione d'impatto sulla protezione dei dati, come esposto nel paragrafo 5. VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI.

3.9. Gestione delle violazioni dei dati personali

3.9.1. Cosa dice la normativa

3.9.1.1. Art.33: Notifica di una violazione dei dati personali all'autorità di controllo

Articolo 33 del Regolamento

1. **In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo** competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, **entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche**. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

3. La notifica di cui al paragrafo 1 deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

3.9.1.2. Art.34: Comunicazione di una violazione dei dati personali all'interessato

Articolo 34 del Regolamento

1. **Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato** senza ingiustificato ritardo.

2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33 (vedi 3.9.1.1. Art.33: Notifica di una violazione dei dati personali all'autorità di controllo), paragrafo 3, lettere b), c) e d).

3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

3.9.2. Interpretazioni

In base al considerando 85, una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.
Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, ovvero il Garante, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Ad esempio la segnalazione al Garante può essere effettuata attraverso la compilazione del modulo disponibile al seguente link (attenzione, è richiesto l'utilizzo della firma digitale):

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1915835

e la trasmissione del modulo compilato al Garante attraverso posta elettronica certificata all'indirizzo protocollo@pec.gpdp.it

In base al considerando 86, il titolare del trattamento dovrebbe comunicare all'interessato la violazione dei dati personali senza indebito ritardo, qualora questa violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà della persona fisica, al fine di consentirgli di prendere le precauzioni necessarie.
La comunicazione dovrebbe descrivere la natura della violazione dei dati personali e formulare raccomandazioni per la persona fisica interessata intese ad attenuare i potenziali effetti negativi. Tali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti quali le autorità incaricate dell'applicazione della legge. Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione agli interessati fosse tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni di dati personali ripetute o analoghe potrebbe giustificare tempi più lunghi per la comunicazione.

3.10. Autorità di controllo

3.10.1. Cosa dice la normativa

3.10.1.1. Art.51: Autorità di controllo

Articolo 51 del Regolamento

1. 1. Ogni Stato membro dispone che una o più **autorità pubbliche indipendenti siano incaricate di controllare l'applicazione del presente regolamento** al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione (**«autorità di controllo»**).

2. *Omissis*.

3. *Omissis*.

4. *Omissis*.

3.10.1.2. Art. 2-bis del Decreto 101/2018: Autorità di controllo

Articolo 2-bis del Decreto 101/2018

1. **L'Autorità di controllo** di cui all'articolo 51 del regolamento è individuata nel **Garante per la protezione dei dati personali**, di seguito "Garante", di cui all'articolo 153.

3.10.1.3. Art.58: Poteri dell'autorità di controllo

Articolo 58 del Regolamento

1. Ogni autorità di controllo ha tutti i **poteri di indagine** seguenti:

a) ingiungere al titolare del trattamento e al responsabile del trattamento e, ove applicabile, al rappresentante del titolare del trattamento o del responsabile del trattamento, di fornirle ogni informazione di cui necessiti per l'esecuzione dei suoi compiti;
b) condurre indagini sotto forma di attività di revisione sulla protezione dei dati;
c) effettuare un riesame delle certificazioni rilasciate in conformità dell'articolo 42, paragrafo 7;
d) notificare al titolare del trattamento o al responsabile del trattamento le presunte violazioni del presente regolamento;
e) ottenere, dal titolare del trattamento o dal responsabile del trattamento, l'accesso a tutti i dati personali e a tutte le informazioni necessarie per l'esecuzione dei suoi compiti; e
f) ottenere accesso a tutti i locali del titolare del trattamento e del responsabile del trattamento, compresi tutti gli strumenti e mezzi di trattamento dei dati, in conformità con il diritto dell'Unione o il diritto processuale degli Stati membri.

2. Ogni autorità di controllo ha tutti i **poteri correttivi** seguenti:

a) rivolgere avvertimenti al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono verosimilmente violare le disposizioni del presente regolamento;
b) rivolgere ammonimenti al titolare e del trattamento o al responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del presente regolamento;
c) ingiungere al titolare del trattamento o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i diritti loro derivanti dal presente regolamento;
d) ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del presente regolamento, se del caso, in una determinata maniera ed entro un determinato termine;
e) ingiungere al titolare del trattamento di comunicare all'interessato una violazione dei dati personali;
f) imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento;
g) ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento a norma degli articoli 16 (vedi 3.4.1.3. Art.16: Diritto di rettifica), 17 (vedi 3.4.1.4. Art.17: Diritto alla cancellazione («diritto all'oblio»)) e 18 (vedi 3.4.1.5. Art.18: Diritto di limitazione di trattamento) e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali ai sensi dell'articolo 17 (vedi 3.4.1.4. Art.17: Diritto alla cancellazione («diritto all'oblio»)), paragrafo 2, e dell'articolo 19 (vedi 3.4.1.6. Art.19: Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento);
h) revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti;
i) infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83 (vedi 3.11.1.4. Art.83: Condizioni generali per infliggere sanzioni amministrative pecuniarie), in aggiunta alle misure di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso; e
j) ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale.

3. Ogni autorità di controllo ha tutti i poteri autorizzativi e consultivi seguenti:

a) fornire consulenza al titolare del trattamento, secondo la procedura di consultazione preventiva di cui all'articolo 36 (vedi 3.8.1.2. Art.35,36: Valutazione d'impatto e consultazione preventiva);
b) omissis
c) omissis
d) omissis
e) omissis
f) rilasciare certificazioni e approvare i criteri di certificazione conformemente all'articolo 42, paragrafo 5;
g) omissis
h) autorizzare le clausole contrattuali di cui all'articolo 46 (vedi 3.6.1.3. Art.46: Trasferimento soggetto a garanzie adeguate), paragrafo 3, lettera a);
i) autorizzare gli accordi amministrativi di cui all'articolo 46 (vedi 3.6.1.3. Art.46: Trasferimento soggetto a garanzie adeguate), paragrafo 3, lettera b);
j) approvare le norme vincolanti d'impresa ai sensi dell'articolo 47 (vedi 3.6.1.4. Art.47: Norme vincolanti d'impresa).

4. *Omissis*

5. *Omissis*

6. *Omissis*

3.10.1.4. Art. 157 del Decreto 101/2018: Richiesta di informazioni e di esibizione di documenti

Articolo 157 del Decreto 101/2018

1. Nell'ambito dei poteri di cui all'articolo 58 del Regolamento, e per l'espletamento dei propri compiti, il Garante puo' richiedere al titolare, al responsabile, al rappresentante del titolare o del responsabile, all'interessato o anche a terzi di fornire informazioni e di esibire documenti anche con riferimento al contenuto di banche di dati.

3.11. Mezzi di ricorso, responsabilità e sanzioni

3.11.1. Cosa dice la normativa

3.11.1.1. Art.77 del Regolamento e Art.141 del Decreto 101/2018: Diritto di proporre reclamo all'autorità di controllo

Articolo 77 del Regolamento

1. 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.

2. L'autorità di controllo a cui è stato proposto il reclamo informa il reclamante dello stato o dell'esito del reclamo, compresa la possibilità di un ricorso giurisdizionale ai sensi dell'articolo 78.

Art. 141 del Decreto 101/2018: Reclamo al Garante

1. L'interessato puo' rivolgersi al Garante mediante reclamo ai sensi dell'articolo 77 del Regolamento.

3.11.1.2. Art.79: Diritto a un ricorso giurisdizionale effettivo nei confronti del titolare del trattamento o del responsabile del trattamento

Articolo 79 del Regolamento

1. Fatto salvo ogni altro ricorso amministrativo o extragiudiziale disponibile, compreso il diritto di proporre reclamo a un'autorità di controllo ai sensi dell'articolo 77 (vedi 3.11.1.1. Art.77 del Regolamento e Art.141 del Decreto 101/2018: Diritto di proporre reclamo all'autorità di controllo), **ogni interessato ha il diritto di proporre un ricorso giurisdizionale** effettivo qualora ritenga che **i diritti di cui gode a norma del presente regolamento siano stati violati** a seguito di un trattamento.

2. Le azioni nei confronti del titolare del trattamento o del responsabile del trattamento sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui il titolare del trattamento o il responsabile del trattamento ha uno stabilimento. In alternativa, tali azioni possono essere promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'interessato risiede abitualmente, salvo che il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica di uno Stato membro nell'esercizio dei pubblici poteri.

3.11.1.3. Art.82: Diritto al risarcimento e responsabilità

Articolo 82 del Regolamento

1. **Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento** del danno dal titolare del trattamento o dal responsabile del trattamento.

2. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.

3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

4. Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.

5. Qualora un titolare del trattamento o un responsabile del trattamento abbia pagato, conformemente al paragrafo 4, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno conformemente alle condizioni di cui al paragrafo 2.

6. Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79 (vedi 3.11.1.2. Art.79: Diritto a un ricorso giurisdizionale effettivo nei confronti del titolare del trattamento o del responsabile del trattamento), paragrafo 2.

3.11.1.4. Art.83: Condizioni generali per infliggere sanzioni amministrative pecuniarie

Articolo 83 del Regolamento

1. Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte ai sensi del presente articolo in relazione alle violazioni del presente regolamento di cui ai paragrafi 4, 5 e 6 siano in ogni singolo caso effettive, proporzionate e dissuasive.

2. Le sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso, in aggiunta alle misure di cui all'articolo 58 (vedi 3.10.1.3. Art.58: Poteri dell'autorità di controllo), paragrafo 2, lettere da a) a h) e j), o in luogo di tali misure. Al momento di decidere se infliggere una **sanzione amministrativa pecuniaria** e di fissare l'ammontare della stessa in ogni singolo caso **si tiene debito conto dei seguenti elementi**:

a) la **natura, la gravità e la durata della violazione** tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il **numero di interessati lesi** dal danno e il livello del **danno da essi subito**;
b) il **carattere doloso o colposo della violazione**;
c) le **misure adottate** dal titolare del trattamento o dal responsabile del trattamento **per attenuare il danno** subito dagli interessati;
d) il **grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative** da essi messe in atto ai sensi degli articoli 25 (vedi 3.8.1.3. Art.25: Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita) e 32 (vedi 3.8.1.1. Art.32: Misure di sicurezza tecniche e organizzative);
e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;
f) il **grado di cooperazione con l'autorità di controllo** al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;
g) le **categorie di dati personali** interessate dalla violazione;
h) la **maniera in cui l'autorità di controllo ha preso conoscenza della violazione**, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;
i) qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58 (vedi 3.10.1.3. Art.58: Poteri dell'autorità di controllo), paragrafo 2 (*n.d.r. poteri correttivi dell'autorità di controllo*), nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;
j) l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42; e
k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

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

4. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a **sanzioni amministrative pecuniarie fino a 10 000 000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente**, se superiore:

a) gli **obblighi del titolare del trattamento e del responsabile del trattamento** a norma degli articoli
    - 8 (vedi 3.3.1.4. Art.8: Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione) ,
    - 11 (vedi 3.3.1.9. Art. 11: Trattamento che non richiede l'identificazione),
    - da 25 a 39 (vedi
        - 3.8.1.3. Art.25: Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita,
        - 3.5.1.2. Art.26: Contitolari del trattamento,

        - *n.d.r. articolo 27 Rappresentanti di titolari o responsabili del trattamento non stabiliti nell'Unione*,
        - 3.5.1.3. Art.28,29: Responsabile del trattamento,
        - 3.7. Art.30: Registri delle attività di trattamento,
        - 3.5.1.5. Art. 31: Cooperazione con l'autorità di controllo,
        - 3.8.1.1. Art.32: Misure di sicurezza tecniche e organizzative,
        - 3.9.1.1. Art.33: Notifica di una violazione dei dati personali all'autorità di controllo,
        - 3.9.1.2. Art.34: Comunicazione di una violazione dei dati personali all'interessato,
        - 3.8.1.2. Art.35,36: Valutazione d'impatto e consultazione preventiva,
        - 3.5.1.4. Art.37,38,39: Responsabile della protezione dei dati (Data Protection Officer)),
    - 42 e 43 (*n.d.r. certificazione*);

b) omissis

c) omissis

5. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a **sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente**, se superiore:

a) i **principi di base del trattamento**, comprese le condizioni relative al consenso, a norma degli articoli
    - 5 (vedi 3.3.1.1. Art.5: Principi applicabili al trattamento di dati personali),
    - 6 (vedi 3.3.1.2. Art.6: Liceità del trattamento),
    - 7 (vedi 3.3.1.3. Art.7: Condizioni per il consenso) e
    - 9 (vedi 3.3.1.6. Art.9: Trattamento di categorie particolari di dati personali);

b) i **diritti degli interessati** a norma degli articoli da 12 a 22 (vedi
    - 3.4.1.10. Art.12: Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato,
    - 3.4.1.1. Art.13,14 del Regolamento e Art.111-bis del Decreto 101/2018: Informazioni all'interessato relative al trattamento dei dati personali,
    - 3.4.1.2. Art.15: Diritto di Accesso,
    - 3.4.1.3. Art.16: Diritto di rettifica,
    - 3.4.1.4. Art.17: Diritto alla cancellazione («diritto all'oblio»),
    - 3.4.1.5. Art.18: Diritto di limitazione di trattamento,
    - 3.4.1.6. Art.19: Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento,
    - 3.4.1.7. Art.20: Diritto alla portabilità dei dati,
    - 3.4.1.8. Art.21: Diritto di opposizione,
    - 3.4.1.9. Art.22: Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione);

c) i **trasferimenti di dati personali a un destinatario in un paese terzo** o un'organizzazione internazionale a norma degli articoli da 44 a 49 (vedi
    - 3.6.1.1. Art.44: Principio generale per il trasferimento,
    - 3.6.1.2. Art.45: Trasferimento sulla base di una decisione di adeguatezza, 3.6.1.3. Art.46: Trasferimento soggetto a garanzie adeguate,
    - 3.6.1.4. Art.47: Norme vincolanti d'impresa,

- *n.d.r. articolo 48 trasferimento o comunicazione non autorizzati dal diritto dell'Unione*,
- 3.6.1.5. Art.49: Deroghe in specifiche situazioni) ;

d) qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX (*n.d.r. disposizioni relative a specifiche situazioni di trattamento*);

e) l'**inosservanza** di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'**autorità di controllo** ai sensi dell'articolo 58 (vedi 3.10.1.3. Art.58: Poteri dell'autorità di controllo), paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1.

6. In conformità del paragrafo 2 del presente articolo, l'inosservanza di un ordine da parte dell'autorità di controllo di cui all'articolo 58 (vedi 3.10.1.3. Art.58: Poteri dell'autorità di controllo), paragrafo 2, è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

7. Fatti salvi i poteri correttivi delle autorità di controllo a norma dell'articolo 58 (vedi 3.10.1.3. Art.58: Poteri dell'autorità di controllo), paragrafo 2, ogni Stato membro può prevedere norme che dispongano se e in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici istituiti in tale Stato membro.

8. *Omissis*

9. Se l'ordinamento giuridico dello Stato membro non prevede sanzioni amministrative pecuniarie, il presente articolo può essere applicato in maniera tale che l'azione sanzionatoria sia avviata dall'autorità di controllo competente e la sanzione pecuniaria sia irrogata dalle competenti autorità giurisdizionali nazionali, garantendo nel contempo che i mezzi di ricorso siano effettivi e abbiano effetto equivalente alle sanzioni amministrative pecuniarie irrogate dalle autorità di controllo. In ogni caso, le sanzioni pecuniarie irrogate sono effettive, proporzionate e dissuasive. Tali Stati membri notificano alla Commissione le disposizioni di legge adottate a norma del presente paragrafo al più tardi entro il 25 maggio 2018 e comunicano senza ritardo ogni successiva modifica.

3.11.1.5. Art. 84: Sanzioni

Articolo 84 del Regolamento

1. Gli Stati membri stabiliscono le norme (*n.d.r. vedi Decreto 101/2018*) relative alle altre sanzioni per le violazioni del presente regolamento in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie a norma dell'articolo 83 (vedi 3.11.1.4. Art.83: Condizioni generali per infliggere sanzioni amministrative pecuniarie), e adottano tutti i provvedimenti necessari per assicurarne l'applicazione. Tali sanzioni devono essere effettive, proporzionate e dissuasive.

2. Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del paragrafo 1 al più tardi entro il 25 maggio 2018, e comunica senza ritardo ogni successiva modifica.

3.11.1.6. Art.166 del Decreto 101/2018: Criteri di applicazione delle sanzioni amministrative pecuniarie e procedimento per l'adozione dei provvedimenti correttivi e sanzionatori

1. Sono soggette alla sanzione amministrativa di cui all'articolo 83 (vedi 3.11.1.4. Art.83: Condizioni generali per infliggere sanzioni amministrative pecuniarie), paragrafo 4 (*n.d.r.* ***fino a 10 000 000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente***), del Regolamento le violazioni delle disposizioni di cui agli articoli

- 2-quinquies (*n.d.r. consenso del minore in relazione ai servizi della società dell'informazione*), comma 2,
- 2-quinquiesdecies (*n.d.r. trattamento che presenta rischi elevati per l'esecuzione di un compito di interesse pubblico*),
- 92 (*n.d.r. Cartelle cliniche*) , comma 1,
- 93 (*n.d.r. certificato di assistenza al parto*), comma 1,
- 123, comma 4 (*n.d.r. informazioni sui dati relativi al traffico di una rete o di un servizio pubblico*),
- 128 (*n.d.r. trasferimento automatico della chiamata di un servizio di comunicazione elettronica accessibile al pubblico*),
- 129, comma 2 *(n.d.r. consenso all'inclusione negli elenchi dei contraenti disponibili al pubblico per finalità di marketing*), e
- 132-ter (*n.d.r. sicurezza del trattamento dei servizi di comunicazione elettronica accessibili al pubblico*).
- Alla medesima sanzione amministrativa è soggetto colui che non effettua la valutazione di impatto di cui all'articolo 110, comma 1, primo periodo, ovvero non sottopone il programma di ricerca a consultazione preventiva del Garante a norma del terzo periodo del predetto comma.

2. Sono soggette alla sanzione amministrativa di cui all'articolo 83 (vedi 3.11.1.4. Art.83: Condizioni generali per infliggere sanzioni amministrative pecuniarie), paragrafo 5 (*n.d.r.* ***fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente***), del Regolamento le violazioni delle disposizioni di cui agli articoli

- 2-ter (*n.d.r. base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*),
- 2-quinquies (*n.d.r. consenso del minore in relazione ai servizi della società dell'informazione*) , comma 1,
- 2-sexies (*n.d.r. trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante*),
- 2-septies (*n.d.r. misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute*), comma 7,
- 2-octies (*n.d.r. principi relativi al trattamento di dati relativi a condanne penali e reati*),
- 2-terdecies (*n.d.r. diritti riguardanti le persone decedute*), commi 1, 2, 3 e 4,
- 52 (*n.d.r. dati identificativi degli interessati*), commi 4 e 5,
- 75 (n.d.r. *specifiche condizioni in ambito sanitario*),
- 78 (*n.d.r. informazioni del medico di medicina generale o del pediatra*),
- 79 (*n.d.r. informazioni da parte di strutture pubbliche e private che erogano prestazioni sanitarie e socio-sanitarie*),

- 80 (*n.d.r. informazioni da parte di altri soggetti*) ,
- 82 (*n.d.r. emergenze e tutela della salute e dell'incolumità fisica*) ,
- 92 (*n.d.r. cartelle cliniche*), comma 2,
- 93 (*certificato di assistenza al parto*), commi 2 e 3,
- 96 (*n.d.r. trattamento di dati relativi a studenti*),
- 99 (*n.d.r. durata del trattamento*),
- 100 (*n.d.r. dati relativi ad attività di studio e ricerca*), commi 1, 2 e 4,
- 101 (*n.d.r. trattamento a fini di archiviazione nel pubblico interesse o di ricerca storica - modalità di trattamento*),
- 105 (*n.d.r. trattamento a fini statistici o di ricerca scientifica - modalità di trattamento*) commi 1, 2 e 4,
- 110-bis (*n.d.r. trattamento ulteriore da parte di terzi dei dati personali a fini di ricerca scientifica o a fini statistici*), commi 2 e 3,
- 111 (*n.d.r. regole deontologiche per trattamenti nell'ambito del rapporto di lavoro*), 111-bis (*n.d.r. informazioni in caso di ricezione di curriculum*),
- 116 (*n.d.r. istituti di patronato e di assistenza sociale*) , comma 1,
- 120 (*n.d.r. altri trattamenti in ambito pubblico o di interesse pubblico*), comma 2,
- 122 (*n.d.r. Comunicazioni elettroniche - informazioni raccolte nei riguardi del contraente o dell'utente*),
- 123 (*n.d.r. Comunicazioni elettroniche - dati relativi al traffico*), commi 1, 2, 3 e 5,
- 124 (*n.d.r. Comunicazioni elettroniche - fatturazione dettagliata*),
- 125 (*n.d.r. Comunicazioni elettroniche - identificativo della linea*),
- 126 (*n.d.r. Comunicazioni elettroniche - dati relativi all'ubicazione*),
- **130 (*n.d.r. Comunicazioni elettroniche - comunicazioni indesiderate*)**, commi da 1 a 5,
- 131 (*n.d.r. Comunicazioni elettroniche - informazioni a contraenti e utenti*),
- 132 (*n.d.r. Comunicazioni elettroniche - conservazione di dati di traffico per altre finalità*),
- 132-bis (*n.d.r. Comunicazioni elettroniche - procedure istituite dai fornitori*), comma 2,
- 132-quater (*n.d.r. comunicazioni elettroniche - informazioni sui rischi*),
- 157 (*n.d.r. richiesta di informazioni e di esibizione di documenti*),
- nonché delle misure di garanzia, delle regole deontologiche di cui rispettivamente agli articoli 2-septies e 2-quater.

3. Il Garante è l'organo competente ad adottare i provvedimenti correttivi di cui all'articolo 58 (vedi 3.10.1.3. Art.58: Poteri dell'autorità di controllo), paragrafo 2, del Regolamento, nonché ad irrogare le sanzioni di cui all'articolo 83 (vedi 3.11.1.4. Art.83: Condizioni generali per infliggere sanzioni amministrative pecuniarie) del medesimo Regolamento e di cui ai commi 1 e 2.

4. Il procedimento per l'adozione dei provvedimenti e delle sanzioni indicati al comma 3 può essere avviato, nei confronti sia di soggetti privati, sia di autorità pubbliche ed organismi pubblici, a seguito di reclamo ai sensi dell'articolo 77 (vedi 3.11.1.1. Art.77 del Regolamento e Art.141 del Decreto 101/2018: Diritto di proporre reclamo all'autorità di controllo) del Regolamento o di attività istruttoria d'iniziativa del Garante, nell'ambito dell'esercizio dei poteri d'indagine di cui all'articolo 58 (vedi 3.10.1.3. Art.58: Poteri dell'autorità di controllo), paragrafo 1, del Regolamento, nonché in relazione ad accessi, ispezioni e verifiche svolte in base a poteri di accertamento autonomi, ovvero delegati dal Garante.

5. L'Ufficio del Garante, quando ritiene che gli elementi acquisiti nel corso delle attività di cui al comma 4 configurino una o più violazioni indicate nel presente titolo e nell'articolo 83 (vedi 3.11.1.4. Art.83: Condizioni generali per infliggere sanzioni amministrative pecuniarie), paragrafi

4, 5 e 6, del Regolamento, avvia il procedimento per l'adozione dei provvedimenti e delle sanzioni di cui al comma 3 notificando al titolare o al responsabile del trattamento le presunte violazioni, nel rispetto delle garanzie previste dal Regolamento di cui al comma 9, salvo che la previa notifica della contestazione non risulti incompatibile con la natura e le finalità del provvedimento da adottare.

6. Entro trenta giorni dal ricevimento della comunicazione di cui al comma 5, il contravventore può inviare al Garante scritti difensivi o documenti e può chiedere di essere sentito dalla medesima autorità.

7. Nell'adozione dei provvedimenti sanzionatori nei casi di cui al comma 3 si osservano, in quanto applicabili, gli articoli da 1 a 9, da 18 a 22 e da 24 a 28 della legge 24 novembre 1981, n. 689; nei medesimi casi può essere applicata la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione, per intero o per estratto, sul sito internet del Garante. *Omissis*.

8. Entro il termine di cui all'articolo 10, comma 3, del decreto legislativo n. 150 del 2011 previsto per la proposizione del ricorso, il trasgressore e gli obbligati in solido possono definire la controversia adeguandosi alle prescrizioni del Garante, ove impartite, e mediante il pagamento di un importo pari alla metà della sanzione irrogata.

9. *Omissis*

10. Le disposizioni relative a sanzioni amministrative previste dal presente codice e dall'articolo 83 del Regolamento non si applicano in relazione ai trattamenti svolti in ambito giudiziario.

3.11.1.7. Art.167 del Decreto 101/2018: Trattamento illecito di dati

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli

- 123 (*n.d.r. comunicazioni elettroniche - dati relativi al traffico*) ,
- 126 (*n.d.r. comunicazioni elettroniche - dati relativi all'ubicazione*) e
- 130 (*n.d.r. comunicazioni elettroniche - comunicazioni indesiderate*)
- o dal provvedimento di cui all'articolo 129 (*n.d.r. comunicazioni elettroniche - elenchi dei contraenti*)

arreca nocumento all'interessato, è punito con la **reclusione da sei mesi a un anno e sei mesi**.

2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trattamento dei dati personali di cui agli articoli

- 9 (vedi 3.3.1.6. Art.9: Trattamento di categorie particolari di dati personali) e
- 10 (vedi 3.3.1.7. Art.10: Trattamento di dati personali relativi a condanne penali e reati) del Regolamento

in violazione delle disposizioni di cui agli articoli

- 2-sexies (*n.d.r. trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante*) e
- 2-octies (*n.d.r. principi relativi al trattamento di dati relativi a condanne penali e reati*),

- o delle misure di garanzia di cui all'articolo 2-septies *(n.d.r. misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute*)
- ovvero operando in violazione delle misure adottate ai sensi dell'articolo 2-quinquiesdecies

arreca nocumento all'interessato, è punito con la **reclusione da uno a tre anni**.

3. Salvo che il fatto costituisca più grave reato, la pena di cui al comma 2 (*n.d.r.* ***reclusione da uno a tre anni***) si applica altresì a chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli 45 (vedi 3.6.1.2. Art.45: Trasferimento sulla base di una decisione di adeguatezza), 46 (vedi 3.6.1.3. Art.46: Trasferimento soggetto a garanzie adeguate) o 49 (vedi 3.6.1.5. Art.49: Deroghe in specifiche situazioni) del Regolamento, arreca nocumento all'interessato.

4. *Omissis*

5. *Omissis*

6. Quando per lo stesso fatto è stata applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa è stata riscossa, la pena è diminuita.

3.11.1.8. Art. 167-bis del Decreto 101/2018: Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala

1. Salvo che il fatto costituisca più grave reato, chiunque **comunica o diffonde** al fine di trarre profitto per sé o altri ovvero al fine di arrecare danno**, un archivio automatizzato** o una parte sostanziale di esso contenente dati personali oggetto di **trattamento su larga scala**, in violazione degli articoli 2-ter, 2-sexies e 2-octies, è punito con la **reclusione da uno a sei anni**.

2. Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, comunica o diffonde, senza consenso, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, è punito con la reclusione da uno a sei anni, quando il consenso dell'interessato è richiesto per le operazioni di comunicazione e di diffusione.

3. Per i reati di cui ai commi 1 e 2, si applicano i commi 4, 5 e 6 dell'articolo 167.

3.11.1.9. Art. 167-ter del Decreto 101/2018: Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala è punito con la reclusione da uno a quattro anni.

2. Per il reato di cui al comma 1 si applicano i commi 4, 5 e 6 dell'articolo 167.

3.11.1.10. Art. 168 del Decreto 101/2018: Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante

1. Salvo che il fatto costituisca più grave reato, chiunque, in un procedimento o nel corso di **accertamenti dinanzi al Garante**, **dichiara o attesta falsamente** notizie o circostanze o produce atti o documenti falsi, è punito con la **reclusione da sei mesi a tre anni**.

2. Fuori dei casi di cui al comma 1, è punito con la reclusione sino ad un anno chiunque intenzionalmente cagiona un'interruzione o turba la regolarità di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti.

3.11.1.11. Art. 170 del Decreto 101/2018: Inosservanza di provvedimenti del Garante

1. Chiunque, essendovi tenuto, **non osserva il provvedimento adottato dal Garante** ai sensi degli articoli 58 (vedi 3.10.1.3. Art.58: Poteri dell'autorità di controllo), paragrafo 2, lettera f) del Regolamento, dell'articolo 2-septies (*n.d.r. misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute*), comma 1, nonché i provvedimenti generali di cui all'articolo 21, comma 1, del decreto legislativo di attuazione dell'articolo 13 della legge 25 ottobre 2017, n. 163 è punito con la **reclusione da tre mesi a due anni**.

3.11.1.12. Art. 171 del Decreto 101/2018: Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori

1. La violazione delle disposizioni di cui agli articoli 4, comma 1, e 8 della legge 20 maggio 1970, n. 300, è punita con le sanzioni di cui all'articolo 38 della medesima legge.

3.11.1.13. Art. 172 del Decreto 101/2018: Pene accessorie

1. La condanna per uno dei delitti previsti dal presente codice importa la pubblicazione della sentenza, ai sensi dell'articolo 36, secondo e terzo comma, del codice penale.

3.11.2. Interpretazioni

3.11.2.1. Sanzioni introdotte dal Regolamento

Il base al considerando 146 del Regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe risarcire i danni cagionati a una persona da un trattamento non conforme al presente regolamento ma dovrebbe essere esonerato da tale responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

Gli interessati dovrebbero ottenere pieno ed effettivo risarcimento per il danno subito.

Qualora i titolari del trattamento o i responsabili del trattamento siano coinvolti nello stesso trattamento, ogni titolare del trattamento o responsabile del trattamento dovrebbe rispondere per la totalità del danno. Tuttavia, qualora essi siano riuniti negli stessi procedimenti giudiziari

conformemente al diritto degli Stati membri, il risarcimento può essere ripartito in base alla responsabilità che ricade su ogni titolare del trattamento o responsabile del trattamento per il danno cagionato dal trattamento, a condizione che sia assicurato il pieno ed effettivo risarcimento dell'interessato che ha subito il danno. Il titolare del trattamento o il responsabile del trattamento che ha pagato l'intero risarcimento del danno può successivamente proporre un'azione di regresso contro altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento.

3.11.2.2. Sanzioni introdotte dal Decreto 101/2018

Gli illeciti penali erano stati completamente omessi dal testo normativo del Regolamento e nelle more del nuovo D.Lgs. 101/18, nell'intervallo di tempo tra la cogenza del Regolamento UE e il 19 settembre 2018, era legittimo attendersi una sorta di abrogazione tacita della facoltà di contestare un reato, consistente dal trattamento illecito dei dati.

Ebbene ciò che pareva del tutto estinto, compie nuovamente il proprio ingresso nel panorama normativo attuale, aggiornato nella versione oggi applicabile.

Il titolo II introduce il novero di quelle condotte che possono essere ascritte fra le fattispecie delittuose, ossia i reati.

Il primo aspetto da cogliere è l'aumento della tipologia di illeciti, rispetto al passato.

I reato attualmente contestabili sono:

- Art. 167 trattamento illecito dei dati;
- Art. 167-bis - Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala.;
- Art. 167-ter - Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala,
- Art. 168 Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante;
- Art. 170 Inosservanza di provvedimenti del Garante
- Art. 171 - Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori;
- Art. 172 Pene accessorie.

L'art. 167 dispone che in caso in cui vi sia un trattamento non autorizzato di dati altrui, che produca un profitto a vantaggio dell'autore della violazione dei dati, dati che abbiano per oggetto il traffico, l'ubicazione, dati degli elenchi e delle telefonate indesiderate, o di dati particolari come quelli sensibili o giudiziari, anche per il trasferimento all'estero degli stessi, è stata prescritta una pena detentiva graduata in ordine alla gravità della condotta e può arrivare sino a tre anni di detenzione. Se poi è stata disposta anche una sanzione amministrativa, laddove corrisposta, la pena detentiva prevista per l'illecito penale è diminuita.

Con gli artt. 167 bis, 167, ter i reati di frode sono completate con condotte quali la diffusione o la comunicazione a terzi, ma anche la acquisizione, non autorizzata, di dati particolari o di dati su larga scala, che siano la totalità o una sola parte di un archivio informatizzato. Le sanzioni, sempre di carattere penale si inaspriscono ulteriormente le pene detentive che arrivano sino a 6 anni di detenzione, escludendo l'applicazione di misure quali la messa alla prova.

Infine si contemplano i reati legati alla inottemperanza di disposizioni di leggi speciali in materia (vd. Controllo a distanza lavoratori), oppure dei provvedimenti e/o delle disposizioni del Garante.

Quanto agli strumenti di tutela l'art. 166 del Codice della Privacy aggiornata dal nuovo D.Lgs. 101/18 ha introdotto il sistema di reclamo per poter contestare una per così dire "non conformità" al Regolamento, indicando anche i criteri per i quali sono applicabili le sanzioni del regolamento UE, secondo l'art. 77 del Regolamento. Il Garante conduce interamente l'iter di accertamento della responsabilità per le violazioni presunte e comunica l'intento di procedere al titolare e al responsabile del trattamento, il quale avrà 30 giorni per trasmettere propri scritti difensivi e documenti, nonchè la richiesta di essere sentito dal Garante. Quest'ultimo terminata la propria istruttoria applicherà le sanzioni del caso. Il provvedimento del Garante contenente la sanzione, poi potrà essere impugnato avanti all'Autorità Giudiziaria con rito del lavoro, proposto, a pena di inammissibilita', entro trenta giorni dalla data di comunicazione del provvedimento o dalla data del rigetto tacito, ovvero entro sessanta giorni se il ricorrente risiede all'estero.

Al Garante spetta anche la definizione delle modalità da impiegare per il procedimento di adozione di provvedimenti o sanzioni, secondo le regole del contraddittorio, dello svolgimento di atti istruttori, verbalizzazione e quanto necessario a generare una vera e propria procedura contenente la fase istruttoria e quella decisoria.

3.12. Entrata in vigore e applicazione

3.12.1. Cosa dice la normativa

3.12.1.1. Entrata in vigore e applicazione del Regolamento

Articolo 99 del Regolamento

Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale dell'Unione europea, ovvero il 24 maggio 2016.

Esso si applica a decorrere da **25 maggio 2018**.

3.12.1.2. Entrata in vigore del Decreto 101/2018

Il provvedimento entra in vigore il **19 settembre 2018**.

4. VALUTAZIONE E GESTIONE DEI RISCHI PER I DIRITTI E LE LIBERTÀ DELLE PERSONE FISICHE

La **valutazione dei rischi è necessaria**, tra l'altro:

1. per **determinare l'adeguatezza delle misure di sicurezza a protezione dei trattamenti di dati personali** (vedi 3.8.1.1. Art.32: Misure di sicurezza tecniche e organizzative),
2. per **determinare la necessità di una valutazione d'impatto sui trattamenti e nella valutazione d'impatto stessa** (vedi 3.8.1.2. Art.35,36: Valutazione d'impatto e consultazione preventiva e 5. VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI),
3. per **determinare la necessità di segnalazione di una violazione di dati personali all'autorità di controllo** (vedi 3.9. Gestione delle violazioni dei dati personali).

La normativa non indica orientamenti specifici per la messa in atto di opportune misure e per dimostrare la conformità da parte del titolare del trattamento o dal responsabile del trattamento in particolare per quanto riguarda l'individuazione del rischio connesso al trattamento, la sua valutazione in termini di origine, natura, probabilità e gravità, e l'individuazione di migliori prassi per attenuare il rischio: **le scelte in materia di gestione del rischio sono responsabilità del titolare del trattamento, secondo il principio di responsabilizzazione** (paragrafo 3.3.1.1. Art.5: Principi applicabili al trattamento di dati personali). Tuttavia in base al considerando 77, il titolare o il responsabile può fare riferimento a orientamenti forniti in particolare mediante codici di condotta approvati, certificazioni approvate, linee guida fornite dal comitato o indicazioni fornite da un responsabile della protezione dei dati.

Nelle valutazioni del rischio per le finalità di cui ai punti 1,2 e 3 possono essere utilizzate metodologie differenti, anche in funzione della criticità della valutazione in oggetto, tuttavia si raccomanda la scelta di metodologie tra loro congruenti.

Inoltre è da sottolineare che **esiste un grado di discrezionalità e soggettività nelle possibili azioni da intraprendere che dipende unicamente dal titolare**. Un titolare prudente adotterà delle misure più onerose e restrittive per garantire un livello di rischio a suo avviso accettabile, mentre un titolare fatalista potrebbe ritenere sufficiente adottare delle misure minime. Per questo motivo è importante **scegliere metodologie, criteri e scale di misurazione diffusi, al fine di rendere il più possibile oggettiva la valutazione del rischio**.

Di seguito è esposta una metodologia di esempio per la valutazione e gestione del rischio, adattamento di quella riportata nelle linee guida *Methodology for Privacy Risk Management* del CNIL al contesto oggetto del presente documento. Tale metodologia risulta congruente con quella utilizzata nel software del CNIL di ausilio alla valutazione d'impatto di cui al paragrafo 5. VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI.

4.1. Il rischio e i suoi scenari

In ambito privacy devono essere considerati solo **i rischi relativi al trattamento dei dati personali che hanno impatto sugli interessati**. Sono escluse dal contesto tutte le conseguenze di una potenziale violazione di dati personali che interessano il titolare del trattamento, il responsabile del trattamento, ecc., come ad esempio il rischio di una sanzione.

Il ***rischio*** è la potenzialità che una ***minaccia*** si concretizzi in un ***evento temuto.***

In particolare l'*Articolo 32* del Regolamento (vedi 3.8.1.1. Art.32: Misure di sicurezza tecniche e organizzative) invita a tener conto in special modo dei **rischi** presentati dal trattamento individuando gli ***eventi temuti*** come il risultato di un'azione accidentale o illegale che porta a

- **divulgazione non autorizzata** o accesso a dati personali**,**
- **modifica non autorizzata** di dati personali o di trattamenti,
- **distruzione** o **perdita** di dati personali o indisponibilità di trattamenti.

Lo ***scenario di rischio*** descrive dunque la minaccia e l'evento temuto in cui può concretizzarsi.

Esempio di scenario di rischio. Un professionista tratta dati anagrafici di clienti ai fini di fatturazione; i dati in questione sono conservati in una cartella del PC condivisa in rete priva di password, il PC è connesso ad Internet attraverso un router/firewall che espone su internet un'interfaccia di configurazione la cui password di accesso impostata è quella di fabbrica. Si valuta la minaccia che un attaccante senza specifico fine si introduca nella rete del PC e divulghi i dati personali contenuti nella cartella di rete condivisa.

4.2. Probabilità di rischio: capacità delle sorgenti di rischio e vulnerabilità degli asset

Affinchè un evento temuto si verifichi deve esserci una o più **sorgente di rischio** che causa l'evento, in modo deliberato o accidentale. Le sorgenti di rischio nell'ambito del trattamento di dati personali possono ad esempio essere

- persone che appartengono all'organizzazione: dipendenti, collaboratori, ecc.
- persone esterne all'organizzazione: fornitori, concorrenti, terze parti, ecc.
- risorse non umane: virus informatici, disastri naturali, ecc.

Nello scenario di esempio la sorgente di rischio della minaccia è un attaccante esterno all'organizzazione senza specifico fine.

Le capacità delle sorgenti di rischio di sfruttare le vulnerabilità e concretizzare la minaccia devono essere stimate per ogni minaccia e possono dipendere da

- competenze,
- tempo disponibile,
- risorse finanziarie,
- vicinanza al sistema target,
- motivazione,
- sensazione di impunità, ecc.

Il ***livello di capacità delle sorgenti di rischio*** di concretizzare la minaccia è risultato di una stima, effettuata ad esempio in base alla seguente scala.

Livello	Descrizione livello	Descrizione capacità sorgenti di rischio
1	**Trascurabile**	Le sorgenti di rischio non sembrano avere speciali capacità per portare avanti una minaccia
2	**Limitato**	Le sorgenti di rischio hanno limitate capacità per portare avanti una minaccia
3	**Significante**	Le sorgenti di rischio hanno reali e significanti capacità per portare avanti una minaccia
4	**Massimo**	Le sorgenti di rischio hanno illimitate capacità per portare avanti una minaccia

Nello scenario di esempio l'attaccante non ha specifico fine e pertanto particolare motivazione di accedere ai dati. Tuttavia i tentativi di intrusione nelle reti private attraverso router configurati con le impostazioni di fabbrica sono piuttosto diffusi anche a causa delle difficoltà di individuazione e sanzione del colpevole e della riconosciuta disponibilità di tool per il recupero della password di fabbrica, pertanto si può stimare che la sorgente di rischio abbia Significative capacità.

La sorgente di rischio agisce sul dato, accidentalmente o deliberatamente attraverso uno o più beni, anche definiti **asset di supporto**, che possono includere:

- hardware e software: computers, chiavette USB, hard disk esterni, ecc.; sistemi operativi, programmi, database, ecc.
- reti di dati: reti ethernet, reti wireless, rete internet, ecc.
- supporti cartacei: stampe, fotocopie, ecc.
- canali di trasmissione della carta: posta cartacea, canali di smaltimento della carta, ecc.

Nello scenario di esempio gli asset di supporto sono due, la rete di dati e il PC.

La minaccia è diretta ad obiettivo ed è concretizzabile se esiste almeno una ***vulnerabilità*** negli asset a supporto del trattamento dei dati che può essere sfruttata dalla minaccia.

Il ***livello di vulnerabilità*** di un asset è risultato di una stima, che può essere ad esempio effettuata in base alla seguente scala.

Livello	Descrizione livello	Descrizione vulnerabilità	Esempio
1	**Trascurabile**	Non sembra possibile che una minaccia si concretizzi sfruttando le vulnerabilità degli asset di supporto	Furto di documenti caratacei conservati in una stanza protetta da lettore di badge e codice d'accesso
2	**Limitato**	Sembra difficile che una minaccia si concretizzi sfruttando le vulnerabilità degli asset di supporto	Furto di documenti caratacei conservati in una stanza protetta da lettore di badge
3	**Significativo**	Sembra possibile che una minaccia si concretizzi sfruttando le vulnerabilità degli asset di supporto	Furto di documenti caratacei conservati in una stanza accessibile solo previo controllo alla reception
4	**Massimo**	Sembra estremamente facile che una minaccia si concretizzi sfruttando le vulnerabilità degli asset di supporto	Furto di documenti caratacei conservati in una stanza accessibile al pubblico

Nello scenario di esempio le vulnerabilità evidenti sono due: la cartella di rete condivisa priva di password di accesso ed il router la cui password di accesso è quella di fabbrica. Considerando che in internet sono disponibili tool per calcolare la password di fabbrica di molti router in commercio, e che i dati personali sono direttamente accessibili dalla rete, il livello di vulnerabilità si può stimare come Significativo.

Tanto maggiore è la capacità delle sorgenti di rischio e l'entità della vulnerabilità dell'obiettivo tanto maggiore è la ***probabilità*** che la minaccia si concretizzi: il livello di probabilità può essere ad esempio il risultato della funzione sotto riportata applicata sul livello della capacità delle sorgenti di rischio e sul livello delle vulnerabilità dell'obiettivo.

Livello di capacità delle sorgenti di rischio + vulnerabilità degli asset di supporto	Livello di probabilità
<5	**1. Trascurabile**
=5	**2. Limitato**
=6	**3. Significativo**
>6	**4. Massimo**

Nello scenario di esempio la capacità delle sorgenti di rischio risulta di livello 3 (Significativo) e la vulnerabilità risulta di livello 3 (Significativo): il valore totale pertanto risulta 3+3=6 e il livello di probabilità di rischio è Significativo.

4.3. Gravità di rischio: identificabilità ed effetti pregiudizievoli sull'interessato

L'evento temuto in cui si può concretizzare la minaccia ha delle conseguenze di una certa ***gravità***.

In base al considerando 75, **i danni che contribuiscono alla gravità dell'evento temuto possono essere fisici, materiali o immateriali**, in particolare: discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, o qualsiasi altro danno economico o sociale significativo; impedimento sugli interessati dell'esercizio del controllo sui dati personali che li riguardano; valutazione di aspetti personali, in particolare mediante l'analisi o la previsione 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, al fine di creare o utilizzare profili personali. Il **danno è tanto più grave quando riguarda persone fisiche vulnerabili**, in particolare minori o interessa una notevole quantità di dati personali e un vasto numero di interessati. In base al considerando 91, di particolare gravità risultano inoltre gli impatti se i dati sono trattati per adottare decisioni riguardanti determinate persone fisiche in seguito a una valutazione sistematica e globale di aspetti personali relativi alle persone fisiche, basata sulla **profilazione** di tali dati, o in seguito al **trattamento di categorie particolari di dati personali**, dati biometrici o **dati relativi a condanne penali e reati** o a connesse misure di sicurezza; tanto da rendere consigliata una valutazione d'impatto prima di iniziare il trattamento (vedi 3.8.1.2. Art.35,36: Valutazione d'impatto e consultazione preventiva).

Il livello di gravità dell'evento temuto può essere dunque il risultato di una stima effettuata in base ad una scala o il risultato di una funzione applicata su diversi parametri.

Uno dei parametri presi in considerazione per la valutazione gravità dell'evento temuto è l'***identificabilità*** dell'interessato in base ai dati trattati.

In base al considerando 26 del Regolamento, per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici.

Il livello di identificabilità dell'interessato può essere stimato ad esempio in base alla seguente scala:

Livello	Descrizione livello	Descrizione identificabilità	Esempio
1	**Trascurabile**	Identificare un individuo dai suoi dati personali appare virtualmente impossibile	Individuare il soggetto tra tutta la popolazione italiana utilizzando il suo nome di battesimo
2	**Limitato**	Identificare un individuo dai suoi dati personali appare difficile ma possibile in certi casi	Individuare il soggetto tra tutta la popolazione italiana utilizzando il suo nome e cognome
3	**Significativo**	Identificare un individuo dai suoi dati personali appare relativamente facile	Individuare il soggetto tra tutta la popolazione italiana utilizzando il suo nome, cognome e data di nascita
4	**Massimo**	Identificare un individuo dai suoi dati personali appare estremamente facile	Individuare il soggetto tra tutta la popolazione italiana utilizzando il suo nome, cognome, data di nascita e indirizzo e-mail oppure foto e indirizzo e-mail

Nello scenario di rischio di esempio il livello di identificabilità dell'interessato è Massimo, in quanto sono trattati i dati anagrafici dell'interessato.

L'altro parametro che concorre alla gravità dell'evento temuto è l'entità degli ***effetti pregiudizievoli*** sull'interessato, ovvero l'entità del danno causato da tutte i potenziali impatti del concretizzarsi dell'evento temuto. Gli effetti pregiudizievoli possono essere stimati ad esempio in base alla seguente scala:

Livello	Descrizione livello	Descrizione generica degli impatti diretti e indiretti
1	**Trascurabile**	Gli interessati non saranno danneggiati o al massimo potrebbero andare incontro a qualche inconveniente, che supereranno senza difficoltà.
2	**Limitato**	Gli interessati potrebbero andare incontro ad inconvenienti significanti, che supereranno nonostante qualche difficoltà.
3	**Significativo**	Gli interessati potrebbero andare incontro a conseguenze significanti, che dovrebbero riuscire a superare nonostanti reali e serie difficoltà
4	**Massimo**	Gli interessati potrebbero andare incontro a conseguenze significanti o addirittura irreversibili, che possono risultare insuperabili

Di seguito un esempio di stima degli **effetti pregiudizievoli rispetto all'impatto materiale sulla persona.**

Livello	Descrizione livello	Esempi di impatto materiale sulla persona
1	**Trascurabile**	Perdita di tempo nel ripetere formalità o nell'attesa che queste vengano soddisfatte. Ricezione di e-mail indesiderate (spam). Riutilizzo di dati pubblicati su siti web (es. social network) per inviare comunicazioni pubblicitarie via posta cartacea.
2	**Limitato**	Pagamenti non preventivati (es. imposti erroneamente), costi aggiuntivi (es. spese bancarie, spese legali), mancati pagamenti. Mancanza di accesso a servizi amministrativi o commerciali. Opportunità perse relative a comodità (es. cancellazione di attività di svago, di ordini, vacanze, chiusura di account on-line). Mancate promozioni di carriera. Blocco di account on-line (es. giochi, amministrazione). Ricezione di e-mail indesiderate che possono danneggiare la reputazione di interessati. Aumento di costi (ad es. polizze assicurative). Mancato aggiornamento di dati (es. posizione lavorativa precedentemente occupata). Trattamento di dati errati che causano ad esempio malfunzionamenti agli account (es. banche, organizzazioni, ecc.). Pubblicità on-line su aspetti privati che l'individuo desidera mantenere confidenziali (es. gravidanza, tossicodipendenza, alcolismo, ecc.)
3	**Significativo**	Perdite di denaro non compensate. Difficoltà finanziarie permanenti (es. necessità di richiedere un prestito). Specifiche, uniche e non ricorrenti perdite di opportunità (es. non concessione di mutui, non ammissione agli studi, perdita di borse di studio o mancata assunzione). Divieto nel possedere conti correnti bancari. Danni alla proprietà. Perdita de domicilio. Perdita dell'impiego. Separazione o divorzio. Perdita finanziaria a seguito di frode (es. tentativo di phishing). Divieto di espatrio. Perdita dei clienti.
4	**Massimo**	Rischi finanziari. Debiti sostanziali. Inabilità al lavoro. Impossibilità di trasferimento. Perdita di evidenze in contesto giudiziario. Mancato accesso a infrastrutture critiche (es. acqua, elettricità, riscaldamento).

Di seguito un esempio di stima degli **effetti pregiudizievoli rispetto all'impatto psicologico sulla persona.**

Livello	Descrizione livello	Esempi di impatto psicologico sulla persona
1	**Trascurabile**	Fastidio dovuto alla ricezione di informazioni non richieste o al mancato ricevimento di informazioni richieste. Paura di perdere il controllo sui propri dati. Sensazione di intrusione nella vita privata senza danno oggettivo (es. comunicazioni commerciali). Perdita di tempo nell'eseguire configurazioni. Mancato rispetto della libertà della persona nell'accedere a siti commerciali (es. accesso vietato a informazioni sull'alcol dovuto ad registrazione errata dell'età di una persona).
2	**Limitato**	Rifiuto a continuare ad usare sistemi informativi (es. social network). Minori ma oggettivi danni psicologici (diffamazione, danni alla reputazione). Problemi relazionali in ambito personale e lavorativo (es. danni d'immagine, reputazione rovinata, perdita di riconoscimento). Sensazione di invasione della vita privata con danni minori ma non irreversibili. Intimidazione sui social network.
3	**Significativo**	Malesseri psicologici gravi (es. depressione, ansie e fobie). Sensazione di invasione della vita privata con danni irreversibili. Sensazione di vulnerabilità a seguito di citazione in giudizio. Sensazione di violazione dei diritti fondamentali per l'uomo (es. discriminazione, libertà di espressione). Essere vittima di ricatti, intimidazioni, estorsioni, cyberbullismo, molestie, sessuali e non.
4	**Massimo**	Malesseri psicologici di lunga durata o permanenti. Condanne penali. Sequestri di persona. Perdita di legami familiari. Impossibilità di far causa. Perdita dell'autonomia legale (sottoposizione a custodia legale).

Di seguito un esempio di stima degli **effetti pregiudizievoli rispetto all'impatto fisico sulla persona**.

Livello	Descrizione livello	Esempi di impatto fisico sulla persona
1	**Trascurabile**	Mancanza di cura adeguata a persona dipendente dagli altri (minore o persona in custodia) che. Mal di testa transitori.
2	**Limitato**	Malesseri fisici minori (ad es. malattie fisiche minori dovute all' inosservanza di cointroindicazioni). Mancanza di cura che porta a minori ma reali danni. Diffamazione che porta a conseguenze minori fisiche o psicologiche.
3	**Significativo**	Malesseri fisici fisiche che causano danni permanenti alla salute (es. peggioramento della salute dovuta a cure improprie o all'inosservanza di controindicazioni). Alterazione dell'integrità fisica, ad es. a seguito di aggressione, incidenti a casa e al lavoro.
4	**Massimo**	Malesseri fisici di lunga durata o permanenti (ad es. dovuti all'inosservanza di cointroindicazioni). Morte (ad es. per suicidio, omicidio o incidente). Disabilità permanente.

Nello scenario di rischio di esempio sono trattati unicamente dati anagrafici, pertanto gli impatti materiali, psicologici e fisici sono da considerarsi Trascurabili, come quindi gli effetti pregiudizievoli sull'interessato.

La gravità di rischio dipende dagli effetti pregiudizievoli sull'interessato e, quando pertinente, dall'identificabilità dell'interessato. Ad esempio in caso l'evento temuto consista nella divulgazione non autorizzata di dati personali, l'identificabilità dell'interessato può rappresentare un fattore determinante della gravità del rischio; invece se si considera la perdita di dati personali a causa di un incendio accidentale l'identificabilità dell'interessato di norma non influisce sulla gravità del rischio.

Pertanto il ***livello di gravità del rischio*** può essere ad esempio pari, in alcuni casi, al livello degli effetti pregiudizievoli sull'interessato ed in altri è invece funzione del livello d'identificabilità ed effetti pregiudizievoli sull'interessato secondo quanto sotto esposto

Livello di identificabilità + effetti pregiudizievoli	Livello di gravità
<5	**1. Trascurabile**
=5	**2. Limitato**
=6	**3. Significativo**
>6	**4. Massimo**

Nello scenario di rischio di esempio il livello di identificabilità è 4 (Massimo) mentre il livello degli effetti pregiudizievoli è 1 (Trascurabile) , come quindi gli effetti pregiudizievoli sull'interessato. Pertanto il valore totale è pari a 1+4=5, e il livello di gravità di rischio è Limitato.

4.4. Il livello di rischio e soglia di accettabilità

Il **rischio** è tanto più alto quanto è **grave** l'evento temuto e **probabile** che la minaccia si concretizzi. il ***livello di rischio*** è il risultato di una funzione applicata sul livello di probabilità della minaccia e sul livello di gravità dell'evento temuto, descritta ad esempio dalla seguente ***mappa del rischio***:

Livello di gravità					
	Massimo	***Significativo***	***Significativo***	***Massimo***	***Massimo***
	Significativo	***Significativo***	***Significativo***	***Massimo***	***Massimo***
	Limitato	***Trascurabile***	***Trascurabile***	***Limitato***	***Limitato***
	Trascurabile	***Trascurabile***	***Trascurabile***	***Limitato***	***Limitato***
Livello di rischio		Trascurabile	Limitato	Significativo	Massimo

Livello di probabilità

Nello scenario di esempio il livello di probabilità di rischio risulta Significativo e il livello di gravità Limitato, pertanto il livello di rischio dello scenario risulta Limitato.

Di seguito un esempio di definizione della ***soglia di accettabilità del rischio***: la soglia di accettabilità del rischio è, come del resto tutta la metodologia di valutazione del rischio, a discrezione del titolare del trattamento, secondo il principio di responsabilizzazione.

	Livello	Descrizione livello	Accettabilità e trattamento del rischio
	1	**Trascurabile**	Il rischio risulta accettabile
	2	**Limitato**	Il rischio risulta accettabile, tuttavia è consigliato adottare misure per ridurre la probabilità
Soglia di accettabilità del rischio →	3	**Significativo**	Il rischio è sulla soglia dell'accettabilità: dovrebbe essere evitato o ridotto adottando misure per la riduzione della gravità ed eventualmente per la riduzione della probabilità
	4	**Massimo**	Il rischio è oltre la soglia dell'accettabilità: deve obbligatoriamente essere evitato o ridotto adottando misure per la mitigazione della gravità ed eventualmente della probabilità

Nello scenario di esempio il livello di rischio è Limitato, pertanto risulta accettabile, ma sono consigliate misure per la riduzione della probabilità.

4.5. Riduzione del rischio e livello di rischio residuo

Nel paragrafo 6. MISURE DI SICUREZZA A PROTEZIONE DEI DATI PERSONALI sono indicate delle misure di sicurezza a riduzione della gravità e della probabilità di rischio.

Le **misure di sicurezza a riduzione della gravità del rischio descritte agiscono principalmente sull'identificabilità dell'interessato e sulla leggibilità dei dati** da parte delle potenziali sorgenti di rischio; le **misure di sicurezza a riduzione della probabilità descritte agiscono principalmente a risoluzione delle vulnerabilità degli asset** a supporto dei trattamenti di dati personali.

L'adozione di ulteriori misure di sicurezza si rende consigliata o necessaria in funzione del livello di rischio dello scenario.

Una volta implementate misure di sicurezza aggiuntive lo scenario di rischio cambia, pertanto è necessaria un'ulteriore valutazione del rischio per stimare il ***livello di rischio residuo***, al fine di rilevare se il rischio risulta sufficientemente ridotto o risultano necessari ulteriori interventi.

Nello scenario di esempio sono consigliate misure per la riduzione della probabilità, che potrebbero consistere ad esempio nella sostituzione della password dell'interfaccia di accesso al router/firewall con una robusta e nell'impostazione di una password di accesso robusta per la cartella di rete condivisa. Lo scenario cambia: il livello di vulnerabilità degli asset diventa Trascurabile, il livello di probabilità diventa Limitato, ed infine il livello di rischio risulta Trascurabile. Una misura di sicurezza che neutralizza completamente la minaccia in esame evitando il rischio potrebbe invece essere quella di inibire l'accesso da Internet all'interfaccia di configurazione del router/firewall.

5. VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

In base al considerando 84, qualora i trattamenti possano presentare in generale un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento dovrebbe essere responsabile dello svolgimento di una ***valutazione d'impatto sulla protezione dei dati*** per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio. L'esito della valutazione dovrebbe essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta il Regolamento.

In base ai considerando 89 e 91, la valutazione d'impatto si rende necessaria in particolare nei casi seguenti:

- per **trattamenti su larga scala di categorie particolari di dati personali o di dati relativi a condanne penali e a reati**, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati; tuttavia il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato;
- per trattamenti che potenzialmente presentano un rischio elevato, ad esempio, data la loro sensibilità, laddove, in conformità con il grado di conoscenze tecnologiche raggiunto, si utilizzi una **nuova tecnologia su larga scala**, nonché ad altri trattamenti che presentano un rischio elevato per i diritti e le libertà degli interessati, specialmente qualora tali trattamenti rendano più difficoltoso, per gli interessati, l'esercizio dei propri diritti;
- quando i dati sono trattati per adottare decisioni riguardanti determinate persone fisiche in seguito a una **valutazione sistematica e globale di aspetti personali** relativi alle persone fisiche, basata sulla profilazione di tali dati, o in seguito al trattamento di categorie particolari di dati personali, dati biometrici o dati relativi a condanne penali e reati o a connesse misure di sicurezza;
- per la **sorveglianza di zone accessibili al pubblico su larga scala**, in particolare se effettuata mediante dispositivi optoelettronici, o per altri trattamenti che l'autorità di controllo competente ritiene possano presentare un rischio elevato per i diritti e le libertà degli interessati, specialmente perché impediscono a questi ultimi di esercitare un diritto o di avvalersi di un servizio o di un contratto, oppure perché sono effettuati sistematicamente su larga scala.

La valutazione d'impatto, in base all'*Articolo 35* del Regolamento (vedi 3.8.1.2. Art.35,36: Valutazione d'impatto e consultazione preventiva), **contiene** almeno:

a) una **descrizione** sistematica dei **trattamenti** previsti e delle **finalità del trattamento**, compreso, ove applicabile, l'**interesse legittimo perseguito** dal titolare del trattamento;
b) una **valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità**;
c) una **valutazione dei rischi per i diritti e le libertà degli interessati**; e
d) le **misure previste per affrontare i rischi**, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al

presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Esistono **software gratuiti in ausilio alla valutazione d'impatto**: segnalato anche dal Garante, il software del CNIL liberamente scaricabile dal sito *ww.cnil.fr* e disponibile anche in lingua italiana.

In base all'*Articolo 36 del Regolamento* (vedi 3.8.1.2. Art.35,36: Valutazione d'impatto e consultazione preventiva), **il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato** in assenza di misure adottate dal titolare del trattamento per attenuare il rischio. Ad esempio se si utilizza la metodologia di valutazione dei rischi esposta nel paragrafo 4. VALUTAZIONE E GESTIONE DEI RISCHI PER I DIRITTI E LE LIBERTÀ DELLE PERSONE FISICHE, la logica per individuare la necessità di una consultazione preventiva potrebbe essere la valutazione del livello di gravità del rischio.

Infine in base al considerando 95, il responsabile del trattamento, se necessario e su richiesta, dovrebbe assistere il titolare del trattamento nel garantire il rispetto degli obblighi derivanti dallo svolgimento di una valutazione d'impatto sulla protezione dei dati e dalla previa consultazione dell'autorità di controllo.

6. MISURE DI SICUREZZA A PROTEZIONE DEI DATI PERSONALI

La tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del Regolamento.

Al fine di poter dimostrare la conformità con il Regolamento, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati per impostazione predefinita (vedi 3.8.1.3. Art.25: Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita).

Le **misure di sicurezza mitigano, per loro natura, il rischio** sul trattamento dei dati personali (vedi 4.5. Riduzione del rischio e livello di rischio residuo), **agendo**

- **sulla gravità dell'evento temuto**, riducendo ad esempio l'identificabilità o gli effetti pregiudizievoli sull'interessato,
- s**ulla probabilità che la minaccia si concretizzi nell'evento temuto**, riducendo ad esempio le vulnerabilità degli asset di ausilio ai trattamenti,

in relazione ai seguenti eventi temuti

- **divulgazione** non autorizzata o accesso a dati personali**,**
- **modifica** non autorizzata di dati personali o di trattamenti,
- **distruzione o perdita** di dati personali o indisponibilità di trattamenti.

Nello scenario moderno, assume sempre maggior importanza il trattamento dei dati mediante strumenti informatici. L'utilizzo di tali strumenti, tipicamente il personal computer, ha introdotto nuove tipologie di vulnerabilità per i dati in essi contenuti. La maggior parte delle vulnerabilità informatiche, è innescata da errati comportamenti, o mancata applicazione di adeguate misure di sicurezza, molto spesso, a causa della scarsa conoscenza dei rischi e delle contromisure. Nel seguito vengono illustrate, brevemente, le misure più comunemente consigliate, per aumentare il livello di protezione dei dati contenuti in supporti digitali e cartacei e trattati con strumenti informatici e non.

Le misure di sicurezza sono anche riepilogate, con il dettaglio degli eventi temuti che contribuiscono a prevenire, nell'allegato 9.1. GDPR toolkit per i professionisti.

6.1. Misure di sicurezza organizzative

6.1.1. Minimizzazione dei dati

La limitazione della raccolta delle categorie e della quantità di dati personali trattati a quanto necessario alla finalità del trattamento, non solo è un principio fondamentale del Regolamento (vedi 3.3.1.1. Art.5: Principi applicabili al trattamento di dati personali), ma è anche una misura di

sicurezza volta a ridurre l'identificabilità dell'interessato e gli effetti pregiudizievoli sull'interessato stesso, ovvero la gravità del rischio sui trattamenti.

6.1.2. Protezione dell'accesso ai locali

Evidente come la protezione dell'accesso ai locali sia una misura indispensabile per i supporti cartacei, meno evidente il fatto che costituisce una misura di sicurezza anche per i dispositivi elettronici. È molto più facile compromettere un dispositivo, quando se ne ha l'accesso fisico. Gli attacchi mediante intrusione informatica, oltre ad essere molto complessi, in presenza di adeguati dispositivi di sicurezza, hanno lo svantaggio di essere "online". Se occorre molto tempo, è probabile che qualcuno se ne accorga e ponga fine ai tentativi. Viceversa, se un malintenzionato riesce ad appropriarsi di un dispositivo, avrà tutto il tempo che desidera per tentare di violarlo e prendere possesso dei dati in esso contenuti. Per questo, la protezione fisica dei locali contenenti dispositivi informatici è altrettanto e forse anche più importante di quella dei locali contenenti archivi cartacei. Sottrarre un singolo hard disk, peraltro facilmente celabile in tasca, potrebbe equivalere a sottrarre migliaia di faldoni. I locali che ospitano server, dovrebbero sempre essere dotati di misure di sicurezza, e gli accessi consentiti solo al personale addetto e fidato. Sarebbe anche bene che fossero, logisticamente, in posizioni centrali, difficilmente accessibili con la semplice infrazione, per esempio, di una porta o di una finestra.

6.1.3. Idonee misure di sicurezza in viaggio

Quando si trasportano documenti cartacei, ma anche dispositivi contenenti dati, o, comunque, in grado di accedere direttamente ai dati, occorre tenere conto che i rischi aumentano notevolmente. A parte l'ovvio rischio di sottrazione del dispositivo, bisogna anche tenere conto della possibilità di caduta, con conseguente guasto. Possono anche sussistere condizioni che mettano a rischio l'integrità del dispositivo, come temperature molto alte (es. auto al sole) o molto rigide, oppure forti campi elettromagnetici (es. scanner al check in aereo). Tutti questi rischi possono essere mitigati in 2 fasi. Innanzitutto, è necessario disporre sempre di una copia dei dati in un luogo "fisso" sicuro, contro il rischio di guasti. Poi è bene rendere inservibili i dati in caso di furto del dispositivo. Questo è possibile mediante la cifratura, già vista nel caso dei backup, ma che, nel caso di dati "correnti", ha delle implicazioni un po' diverse, che analizzeremo nei prossimi paragrafi.

Un altro aspetto a cui prestare molta attenzione, quando si è in viaggio, è l'accesso a reti WiFi sconosciute. Attraverso queste reti, noi possiamo accedere a dati aziendali, pubblicati attraverso Internet, ma, che gestisce la rete, potrebbe intercettare dati e password a nostra insaputa. Parlando del Cloud vedremo che esistono metodi per scongiurare questa possibilità.

6.1.4. Composizione robusta e scadenza delle password

Le password sono un elemento di sicurezza fondamentale. Oltre a permettere l'accesso ai sistemi operativi, ai software o ai portali di trattamento dei dati, possono concorrere anche alla cifratura dei dati. Chi viene in possesso di un dispositivo e della relativa password, ha l'accesso completo al contenuto di quel dispositivo. Per questo è importante che le password sia "robuste". Esistono numerosi software in grado di "indovinare" le password e, tendenzialmente, utilizzano metodologie di attacco con forza bruta: cioè la prova ripetuta di combinazioni casuali di caratteri, che, con dispositivi opportuni, possono arrivare anche al ritmo di migliaia di miliardi di tentativi al

secondo. L'attacco con forza bruta è ancora più pericoloso quando si avvale dei dizionari, cioè elenchi di password di uso comune. Per esempio, una password composta di 8 cifre, può assumere 100 milioni di possibili valori (si individua in una frazione di secondo), aggiungendo le lettere, si arriva a quasi 3000 miliardi (comunque 1-2 secondi), considerando anche maiuscole, minuscole e i caratteri speciali da tastiera, si arriva a quasi a 3 milioni di miliardi (meno di 1 ora). Tutto questo ci dice che una password di 8 caratteri, con le tecnologie attuali, non è più così sicura. Se la portassi a 10, già servirebbero quasi 6 mesi, rendendo il tentativo vano. Altra cosa da evitare nelle password è che siano riconducibili all'utente (es. indirizzo di casa), perché in questo caso, potrebbe essere indovinata dall'umano, prima che dalla macchina, ed è comunque più vulnerabile agli attacchi di forza bruta che utilizzano come dizionario i dati conosciuti dell'utente.

Altro elemento importante, nel caso, ormai molto frequente, in cui si disponga di accessi a diversi sistemi (soprattutto portali Internet), è quello di non usare la stessa password per servizi diversi. In caso di violazione di un sistema, anche non per nostra colpa, i malintenzionati avrebbero a disposizione una password da provare a tappeto su migliaia di servizi Internet, con il rischio di poter accedere anche ad altri portali non direttamente violati.

Infine è consigliabile cambiare il prima possibile le password assegnate da terzi e quelle di default di tutti i dispositivi: computer, i firewall, dispositivi di rete, NAS, stampanti, inclusi anche quelli meno "sospettabili", come condizionatori, macchinari industriali, ecc. (benché questi ultimi non contengano, né trattino dati, potrebbero divenire veicoli di attacchi ad altri dispositivi).

6.1.5. Idonea custodia delle password

La password è un elemento che ci identifica, come una carta d'identità nel modo digitale. Ciò che viene fatto sui sistemi, utilizzando il nostro nome utente e password, viene, almeno in prima battuta, ricondotto a noi. Sarà poi nostro onere dimostrare che le credenziali ci sono state sottratte: per questo motivo è importantissimo conservarle con estrema cautela.

In particolare occorre evitare di conservare la password su supporti cartacei o elettronici in luoghi dove potrebbe essere facilmente trovata. Possibilmente sarebbe opportuno non scriverla affatto, ma, normalmente, ci si trova ad aver a che fare con decine, se non centinaia, di password ed è umanamente impossibile ricordarle tutte. Ci vengono in aiuto i password manager (molto utilizzato e gratuito il tool KeePass https://keepass.info/), software che permettono di mantenere un archivio cifrato di tutte le nostre password. A questo punto basta ricordare la password di accesso al password manager per poter accedere a tutte le credenziali di autenticazione.

Occorre, infine, sottolineare che è buona norma modificare le password con una certa frequenza (tipicamente qualche mese), anche nel caso in cui si sia ragionevolmente sicuri del fatto che nessuno ne sia venuto a conoscenza.

6.1.6. Gestione delle violazioni della password

Nel caso in cui si venisse a conoscenza del fatto che la nostra password è stata violata, ci si troverebbe di fronte ad un episodio di data breach, che dovrà essere gestito secondo vigente normativa. A parte questo, le misure da prendere immediatamente sono diverse. Innanzitutto, la password deve essere sostituita ovunque sia stata impostata. È necessario, poi, sottoporre a scansioni anti-malware approfondite tutti i dispositivi accessibili con quella password, perché un malintenzionato potrebbe avervi inserito dei metodi di accesso fraudolenti (le cosiddette

back-door). Occorre poi cercare le tracce di utilizzo della password (es. log degli accessi), per cercare di individuare eventuali attività malevole. Infine, occorre prestare attenzione alle attività possibili, compatibilmente con i poteri attribuiti a quella password. Per esempio, la password di un amministratore di sistema potrebbe aver permesso di creare un nuovo utente, rendendo vana la contromisura di sostituzione della password.

6.1.7. 6.1.7.Segretezza della password

La password deve essere strettamente personale, e non deve essere comunicata a terzi. Se si rende necessario l'accesso al nostro sistema, in nostra assenza, è bene che sia stato previsto, in precedenza, un altro utente di accesso diverso dal nostro. Anche le tecniche di cifratura dei sistemi operativi, in genere, prevedono la possibilità di decifratura da parte di più utenti preimpostati nel sistema.

È molto importante anche fare attenzione a non comunicare accidentalmente elementi che possano far risalire alla password o, comunque, aiutare nella sua individuazione. Alcuni malintenzionati usano tecniche di cosiddetto social engineering, in cui vengono effettuate telefonate false, con l'intento di raccogliere elementi utili per la violazione dei sistemi informatici.

6.1.8. Idoneo smaltimento e consegna in assistenza dei dispositivi elettronici

Quando si smaltiscono dispositivi elettronici, o, comunque, nel caso in cui gli stessi debbano essere inviati in assistenza, occorre prestare attenzione al fatto che i dati non vengano trasferiti con il dispositivo. Nel caso dello smaltimento, può essere opportuno distruggere meccanicamente tutti i supporti digitali (tipicamente l'hard disk), oppure cancellarli mediante opportuni software di formattazione approfondita. Occorre evidenziare che, per esempio, la semplice rimozione della partizione di un hard disk, non è un metodo sicuro, in quanto facilmente reversibile.

Se viceversa, si sta inviando il dispositivo in assistenza, ove possibile, sarebbe opportuno rimuovere e trattenere i supporti digitali. Un'altra possibilità è quella di creare un utente limitato, in grado di accedere al sistema operativo (se l'accesso è necessario per le attività di assistenza), ma non di decifrare il disco dati (che dovrà, ovviamente, essere cifrato).

6.1.9. Idonee misure di conservazione e smaltimento della carta

Benché non si tratti di un supporto digitale, la carta, contiene molto spesso dati digitali stampati attraverso una stampante. La prima buona prassi sarebbe quella di evitare di stampare, se non è assolutamente necessario (ci guadagna anche l'ambiente). Ove strettamente necessario, i documenti stampati devono essere conservati con estrema cura, e non lasciati incustoditi, se non sotto chiave. Importante anche evitare di stampare e lasciare i fogli nella vaschetta della stampante per più tempo dello stretto necessario, soprattutto se, come spesso accade negli studi professionali, la stampante si trova in un'area aperta al pubblico (es. sala d'attesa).

Quando il documento dovrà essere smaltito, se contiene dati personali, dovrà essere opportunamente distrutto, in modo che i dati siano illeggibili e non ricostruibili (a prova di

“puzzle”). Sarebbe meglio utilizzare un distruggi-documenti certificato. Particolare attenzione va posta nella prassi, comune in molti uffici, di “riciclare” il lato posteriore delle vecchie stampe. Nel caso in cui la stampa contenga dei dati personali, è opportuno che il “riciclo” avvenga ad opera di chi aveva eseguito la stampa originale, o, comunque, di chi ha titolo per accedere ai dati originali.

6.1.10. Idoneo comportamento durante la navigazione e l’utilizzo della posta elettronica

Come già detto in precedenza, la maggior parte delle violazioni ai dati aziendali, parte da programmi che vengono aperti come allegati di posta elettronica, o scaricati durante la navigazione. Per questo è molto importante prestare la massima attenzione nell’utilizzo di questi strumenti. È importante non fare mai cieco affidamento negli antivirus, antispam, firewall, ecc., perché questi sistemi, per quanto affidabili, non sono infallibili. Prima di aprire l’allegato in un messaggio di posta elettronica, è bene analizzare attentamente il messaggio. Il fatto di conoscere il mittente non è una garanzia, in quanto è estremamente semplice inviare messaggi di posta elettronica a nome di altri, e tutti i malware sfruttano estensivamente questa caratteristica. Attraverso sofisticati algoritmi che incrociano i dati di rubriche sottratte da computer compromessi, molti malware scelgono mittente e destinatario, garantendo un’elevata probabilità che questi si conoscano. Questo induce il destinatario a “fidarsi” del messaggio. Se ci sono dubbi sul contenuto del messaggio o anche solo se non si aspettava alcun allegato, è sempre bene verificare prima con il mittente se il messaggio è legittimo.

Un discorso analogo vale per i collegamenti presenti nei messaggi. In questo caso, oltre alla possibilità di scaricare virus, il rischio è anche quello della frode informatica denominata phishing. Si riceve un messaggio, per esempio dalla propria banca, in cui si viene invitati a verificare qualcosa, cliccando sul link. Se si clicca sul link, si viene indirizzati ad un sito malevolo che presenta una schermata simile a quella della banca, in cui vengono richieste le credenziali. In generale potremmo accorgercene dall’indirizzo mostrato nella barra del browser (che può anche essere molto simile ma non uguale), o dal fatto che la connessione, in genere, non è sicura (non c’è il lucchetto o la barra verde), ma spesso non ci si fa caso. Nei casi più sofisticati, quelle stesse credenziali vengono addirittura passate al vero sito della banca, che ci fa entrare nel nostro conto. In questo modo non ci accorgiamo di nulla, ma il sito malevolo ha già rubato le nostre credenziali che, qualcuno, potrà utilizzare, successivamente, in modo indebito. Sarebbe sempre buona norma non fare click sui collegamenti nei messaggi di posta elettronica, ma entrare nei portali digitando direttamente l’indirizzo nel browser (o prendendolo dai preferiti). Consideriamo però che, come già visto nel paragrafo 6.1.3. Misure di sicurezza in viaggio, se stiamo usando una connessione WiFi sconosciuta, potremmo finire comunque in un sito malevolo.

In linea generale, è comunque bene evitare di accedere a siti non noti e di dubbia reputazione. Per esempio, le categorie di siti in cui più facilmente si possono scaricare malware, sono quelle relative al cosiddetto file sharing, ossia lo scambio di file multimediali in violazione del diritto d’autore (che, per inciso, è anche un reato).

6.1.11. Formazione del personale

L'informazione, sensibilizzazione e formazione del personale è sicuramente da annoverare nelle misure di prevenzione più efficaci per evitare che comportamenti superficiali o negligenti del personale interno all'organizzazione possano minacciare la sicurezza delle informazioni e, quindi, dei dati personali. Il Regolamento impone infatti che tutte le persone che trattano dati personali sotto il controllo del titolare del trattamento debbano essere istruite per farlo (vedi 7.2. (In)formarsi e (in)formare)

6.1.12. Procedure ed istruzioni per il personale

Unitamente alla formazione del personale è opportuno stabilire un sistema di disposizioni interne (procedure, istruzioni, ecc.) che da un lato permetta al personale di ricordare quali sono le linee di comportamento per un corretto trattamento dei dati personali e le conseguenze in caso di inosservanza delle stesse, dall'altro tuteli la Direzione aziendale o dello Studio rispetto ad eventuali azioni illecite eseguite dai dipendenti e dai collaboratori.

6.1.13. Impegni ed istruzioni per i fornitori

Un sistema di contratti con fornitori comprendenti, unitamente alla designazione dei responsabili esterni al trattamento se del caso, regole stabilite contrattualmente sul comportamento da osservare, modalità operative da attuare, impegni alla riservatezza, ecc. favorisce il rispetto delle regole e delle procedure stabilite e consente al titolare di mantenere maggior controllo sulle attività esternalizzate (es. elaborazione buste paga, tenuta della contabilità, outsourcing informatico, ecc.) e sulle attività svolte dai fornitori presso i locali aziendali (es. manutenzione hardware e software, consulenti, ecc.)

Oltre a predisporre contratti "robusti" con i fornitori è importante designare formalmente il personale dell'organizzazione che deve accedere ai dati e svolgere attività su di essi.

Infine la nomina degli *Amministratori di Sistema*, dove esistono persone che in realtà svolgono questo ruolo, responsabilizza maggiormente queste figure e garantisce maggior tutela al titolare del trattamento.

6.2. Misure di sicurezza tecniche

6.2.1. Pseudonimizzazione dei dati

L'articolo 4 del Regolamento (vedi 3.1. Art.4: Definizioni) definisce la pseudonimizzazione come "il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile".

La pseudonimizzazione consiste nella pratica nel

- dividere la componente identificativa del dato personale dalla sua componente sensibile ed attribuire all'interessato uno pseudonimo, che preso da solo non contribuisca ad identificare l'interessato,
- attribuire alle informazioni sensibili lo pseudonimo dell'interessato,
- conservare separatamente i dati identificativi dai dati sensibili.

Un attaccante recupera il dato personale completo solo se riesce ad accedere ad entrambi gli archivi dove sono conservati i dati identificativi e quelli sensibili.

Ad esempio, consideriamo il dato personale *Alice è malata*: un esempio di pseudonimizzazione consiste nel scrivere su un foglio *Alice è 12345678* e su un altro foglio *12345678 è malata*, conservando i due fogli in archivi distinti con chiavi diverse.

Questa tecnica viene spesso utilizzata anche nei sistemi informatici: è buona norma prediligere software o servizi che adottano la pseudonimizzazione dei dati personali.

6.2.2. Cifratura dei dati

La cifratura è una tecnica che trasforma un dato in modo tale da renderlo illeggibile a meno della conoscenza di un segreto, di solito una password. Se un attaccante accede al dato senza conoscere il segreto, non è in grado né di leggerlo né tanto meno di ricondurlo all'interessato.

La cifratura trova impiego in vari contesti, tra cui quelli in seguito descritti.

6.2.2.1. Software e servizi con cifratura dei dati

Alcuni software in commercio, soprattutto quelli candidati al trattamento di dati la cui riservatezza rappresenta un fattore critico, conservano le informazioni in archivi cifrati, accessibili solo previo inserimento della password corretta. Nella scelta dei software da installare sui PC o servizi in cloud destinati al trattamento di dati personali è buona pratica prediligere quelli che implementano la cifratura degli archivi, soprattutto se vengono trattati dati appartenenti a particolari categorie e dati relativi a condanne penali e reati. La presenza di una password di accesso al software o al servizio non è garanzia della cifratura dei dati, consultare il manuale o chiedere informazioni specifiche al produttore per verificare l'effettiva presenza della funzionalità.

6.2.2.2. Cifratura del sistema operativo

La maggior parte dei sistemi operativi moderni, dispone di tecniche di cifratura integrate. In generale, però, è necessario abilitarle. Può sembrare normale pensare che, la mancata conoscenza della password di accesso, prevenga dall'accesso al dispositivo. In generale, però, la password regola solo l'accesso al sistema operativo. Un malintenzionato che venga in possesso del dispositivo, potrebbe smontare l'hard disk (o altra memoria di massa), ed accedervi per mezzo di un altro dispositivo, recuperando tutti i dati, anche senza conoscere (o scoprire) la password. La cifratura del disco, scongiura questa possibilità, perché i dati in esso contenuti, saranno cifrati, qualunque sia il dispositivo a cui venga collegato. Molti moderni dispositivi (in particolare quelli mobili), dispongono di un componente hardware detto TPM (Trusted Protection Module): questo dispositivo contiene una chiave che è unica al mondo e che, combinata con la password dell'utente, genera una chiave di cifratura robusta. In questo modo, i dati sono accessibili solo su quello specifico dispositivo, e solo conoscendo la password dell'utente.

6.2.2.3. Cifratura dei dispositivi rimovibili

La cifratura è particolarmente importante, soprattutto per i dispositivi rimovibili, in quanto tendono ad essere sempre più piccoli e sono facilmente distaccabili dal dispositivo a cui sono collegati. Un malintenzionato potrebbe sottrarre un dispositivo rimovibile in pochi secondi e portarlo con sé senza essere visto. I dispositivi rimovibili possono essere cifrati con le medesime metodologie utilizzate per cifrare il disco del sistema operativo. È possibile decidere di utilizzare il TPM, nel qual caso, il dispositivo rimovibile sarà utilizzabile solo sul PC su cui è stato cifrato, oppure limitarsi alla password, per esempio perché il dispositivo rimovibile deve essere condiviso fra più PC.

6.2.3. Software antivirus e anti-malware

I virus informatici, e similari (malware, spyware, trojan, ecc.), sono programmi per computer, espressamente sviluppati per arrecare danno ai contenuti del computer che ne viene infettato. Inizialmente venivano sviluppati con finalità esclusivamente distruttive; oggi, si assiste sempre più, al proliferare di virus studiati per portare guadagni allo sviluppatore, tipicamente mediante la richiesta di un riscatto per "sbloccare" i dati (ramsonware). La diffusione di virus informatici è un reato penale in quasi tutti i paesi del mondo (in Italia *art. 615 quinquies del Codice Penale*, cui si aggiunge l'art. 640 ter c.p., se accompagnata da frode informatica), ma la percentuale di criminali assicurati alla giustizia è bassissima. Ad oggi, il principale veicolo di diffusione di virus ed altri malware informatici è la posta elettronica. Il virus può essere allegato al messaggio di posta elettronica, o, molto più spesso, essere presente in un collegamento che il messaggio stesso induce a cliccare. Ricevere o scaricare un virus, in sé, non comporta danni, fintanto che lo stesso non viene eseguito o installato. I programmi antivirus e anti-malware, si occupano di verificare la sicurezza di ogni singolo programma, prima che lo stesso venga eseguito, ed a bloccarlo (messa in quarantena), in caso di sospetto virus. I programmi antivirus analizzano i programmi, sulla base di numerosi criteri, di cui, il principale, è la presenza di opportuni pezzi di codice in una lista di virus noti. Per questo motivo, è opportuno, non solo installare un programma antivirus, di primaria diffusione, su ogni PC e server, ma assicurarsi anche che lo stesso venga aggiornato con cadenza almeno giornaliera (l'aggiornamento avviene automaticamente, ma a volte potrebbe non funzionare).

6.2.4. Software firewall/anti-intrusione

In uno scenario in cui qualsiasi PC o Server è dotato di una connessione a Internet, risulta possibile, per un malintenzionato, accedere ai dati digitali, all'insaputa del titolare. Per l'utente comune di un PC, è estremamente difficile accorgersi dell'intrusione, perché non viene presentato nulla a schermo e le tracce lasciate sono poche e nascoste. Anche l'intrusione in sistemi informatici è un reato penale (in Italia *art. 615 ter del Codice Penale*), ma, anche in questo caso, è difficile risalire al responsabile, che, normalmente, maschera la propria identità, facendo "ponte" in paesi extra UE, dove la richiesta di rogatorie è molto difficile.

Come nel caso dei virus, esistono software in grado di proteggere un dispositivo informatico dalle intrusioni, chiamati comunemente firewall. Molto spesso questi strumenti sono accessori al software antivirus (di serie o acquistabili in opzione), e sono, in parte, integrati nei sistemi operativi moderni (personal firewall). Anche questo tipo di software necessita di aggiornamenti

frequenti, perché le logiche di attacco cambiano e gli strumenti di difesa si adeguano di conseguenza.

6.2.5. Aggiornamenti di sicurezza del software

Come già visto per i software antivirus ed anti-intrusione, qualsiasi tipo di software necessita di aggiornamenti periodici, che, l'azienda produttrice, mette a disposizione per sopperire ad eventuali vulnerabilità individuate dopo il rilascio del software stesso. Praticamente nessun software informatico è esente da vulnerabilità di sicurezza, ed un malintenzionato potrebbe sfruttarle per danneggiare o sottrarre dati. Quando i produttori di software rilasciano un aggiornamento di sicurezza, in pratica, rendono disponibile a chiunque dettagli sulla vulnerabilità sanata, utili anche per sfruttarla malevolmente. Per questo motivo è molto importante applicare il prima possibile gli aggiornamenti di sicurezza ai sistemi operativi, ed a qualunque altro software presente sul dispositivo. Quasi tutti i dispositivi permettono di configurare gli aggiornamenti automatici, per garantire sempre la massima protezione. Una nota molto importante è relativa alla durata del supporto che, il produttore del software, garantisce. I programmi più vecchi, spesso, sono fuori dal periodo di supporto, ed eventuali problemi di sicurezza non vengono più risolti. È molto importante verificare che tutti i sistemi operativi ed i programmi utilizzati, godano ancora del supporto e degli aggiornamenti di sicurezza. In caso contrario, è consigliabile sostituire, il prima possibile, il software con uno più recente.

6.2.6. Idonea gestione degli accessi WiFi

Il WiFi costituisce una infrastruttura di rete, con i medesimi privilegi di accesso di una rete cablata, ma con elementi di sicurezza molto inferiori. Per ottenere l'accesso alla rete cablata, è necessario ottenere l'accesso fisico all'armadio di commutazione o ad una presa a muro attiva, mediante un dispositivo dotato di rete cablata. Questa attività, in genere, è difficilmente occultabile. Le reti WiFi, di contro sono, spessissimo, accessibili anche dalla strada, e con dispositivi anche molto piccoli (smartphone). La presenza di una password di accesso al WiFi, benché aiuti, è un falso elemento di sicurezza, perché in caso la rete WIFI sia configurata con protocolli di comunicazione deboli, con le tecniche che abbiamo visto in precedenza (che nel caso del WiFi tengono conto anche del traffico effettuato da dispositivi "leciti", riducendo enormemente i tempi), la password può essere individuata in tempi ragionevoli. Inoltre, la password del WiFi non è personale e, tendenzialmente, non viene mai cambiata, diventando, ben presto, nota a molte persone.

Sarebbe opportuno che le reti WiFi non fossero connesse alla rete aziendale, ma, solo se necessario, vi accedessero attraverso un Firewall (un po' come se l'accesso avvenisse da Internet).

6.2.7. Idonea configurazione dell'accesso a internet

La tendenza odierna è quella di connettere qualsiasi dispositivo ad Internet, a prescindere dal suo utilizzo. In realtà esistono dispositivi (tipicamente server, ma non solo), che non necessitano di essere connessi a Internet. Sarebbe buona prassi individuare le necessità di connessione ad Internet di ciascun dispositivo, ed effettuare (o non effettuare) la connessione dello stesso, con il minimo insieme di privilegi necessari. Ad esempio, per un server, spesso non è necessaria la connessione ad Internet, fatta eccezione per le funzioni a cui è preposto. Per un server di posta

elettronica, ad esempio, si deve abilitare la ricezione e l'invio della posta, la ricezione degli aggiornamenti dei software e degli antivirus, ma è sconsigliato consentire la navigazione del Web. Queste limitazioni, generalmente, possono essere imposte mediante gli strumenti di configurazione del sistema operativo.

6.2.8. Firewall/router

Il Firewall è un dispositivo anti-intrusione, simile a quanto già visto nel paragrafo 6.2.4. Software firewall/anti-intrusione. In questo caso, però, si tratta di un dispositivo di rete fisico, che, a differenza del software, non si prepone di proteggere un unico computer, ma tutta la rete aziendale. È importante dotare la propria rete di un Firewall di primaria diffusione, e di configurarlo opportunamente per minimizzare i punti di esposizione a Internet (le cosiddette porte aperte). In uno scenario ideale, tutte le porte, da Internet verso la rete aziendale, dovrebbero essere chiuse. Spesso, però, è necessario aprirne alcune, per permettere il funzionamento di servizi, come server di posta o siti Internet. È molto importante che la configurazione del Firewall venga fatta tenendo conto delle più recenti linee guida di sicurezza, e che la stessa venga revisionata frequentemente, per rispondere ad eventuali vulnerabilità scoperte in fasi successive. Il firmware del Firewall (cioè il suo sistema operativo) deve essere mantenuto aggiornato, secondo le direttive del produttore. Anche in questo caso, è importante che il produttore garantisca il supporto e gli aggiornamenti di sicurezza. Nel caso di Firewall obsoleti, è consigliabile, sostituirli, il prima possibile, con dispositivi più moderni. I più comuni Firewall, oltre a proteggere dalle intrusioni (dall'esterno verso l'interno), proteggono anche la navigazione dei dispositivi connessi in rete aziendale (dall'interno verso l'esterno), bloccando, per esempio, siti malevoli, prima che possano compromettere la sicurezza informatica. I più moderni Firewall sono dotati di sistemi antivirus, anti-malware, anti-spam, ecc. Inoltre dispongono di dispositivi attivi di protezione dalle intrusioni, cioè non si limitano a chiudere le porte, ma analizzano il traffico digitale, attraverso le porte aperte, alla ricerca di comportamenti malevoli. Infine, dispongono di sistemi di filtro e protezione della navigazione, per bloccare l'accesso a siti malevoli, o appartenenti a determinate categorie potenzialmente pericolose o illegali. Tutti questi servizi attivi devono essere aggiornati molto frequentemente (tipicamente giornalmente) ed in modo automatico. I produttori di Firewall rendono disponibili contratti di aggiornamento di questi servizi, che è opportuno sottoscrivere.

È opportuno sottolineare nel caso si colleghino dispositivi portatili a reti diverse da quella aziendale, il firewall di rete non protegge in questo caso i suddetti dispositivi, che andranno dunque dotati di un software Firewall.

6.2.9. Backup periodici e disaster recovery

Virus, attacchi informatici, ed altri metodi di sabotaggio, non sono gli unici rischi per l'integrità e la disponibilità dei dati. Anche eventi come guasti dei sistemi, catastrofi naturali, o semplicemente, errori umani, commessi in buona fede, possono comportare la modifica non desiderata o addirittura la perdita di dati. Benché i dispositivi critici (server) siano quasi sempre dotati di sistemi di ridondanza dei dati, è comunque necessario eseguire periodicamente delle copie di salvaguardia dei dati stessi (backup). I backup devono essere eseguiti con una frequenza che dipende sia dall'importanza dei dati, che, soprattutto, dalla loro dinamicità. Per esempio, per dati che vengono aggiornati con cadenza mensile, è possibile ipotizzare un backup mensile (coincidente con il giorno di modifica dei dati), mentre per i dati "correnti", cioè sottoposti ad

aggiornamenti continui, è bene pensare ad un backup con cadenza almeno giornaliera. Molto importante anche il tempo di conservazione dei backup. Non è raro che la cancellazione accidentale di una porzione di dati venga scoperta a settimane di distanza dall'evento. In questi casi, un backup recente non aiuterebbe a recuperarli. In generale, è buona norma poter "tornare indietro nel tempo" di almeno 1 mese, possibilmente anche di più (compatibilmente con le capacità dei supporti di archiviazione dei backup). Molto importante è anche eseguire, periodicamente, delle prove di ripristino (restore), cioè simulazioni di recupero dei dati come se fossero stati persi. Questo evita di trovarsi, all'occorrenza, con copie di backup corrotte o incomplete. È importante anche garantire che eventuali eventi disastrosi, come una calamità naturale, che possano compromettere i dispositivi "correnti", non vadano a compromettere anche i supporti di backup. Si possono adottare diverse strategie, dall'asportazione dei supporti di backup (cassette da portare a casa), all'esecuzione delle copie in posizioni fisicamente distanti dagli originali, inclusi i backup in Cloud. Occorre, però, tenere conto del fatto che la "delocalizzazione" delle copie di backup, rispetto all'ambiente fisicamente protetto in cui si trovano, normalmente, i server, può aumentare il rischio di furti. Per questo è bene adottare misure di sicurezza maggiori sui supporti di backup. La maggior parte dei software di backup permette di eseguire la cifratura delle copie. Questa misura genera delle copie illeggibili, a meno di non disporre della chiave di decifratura, generalmente molto complessa e difficilmente identificabile (e, soprattutto, non salvata sui supporti di backup). La cifratura dei dati, anche a norma del Regolamento, rappresenta una forma di protezione idonea alla conservazione dei dati anche in ambienti non sicuri.

Guasti, calamità ed errori, oltre a comportare il rischio di perdita di dati, mitigato, come abbiamo visto, dalla corretta gestione dei backup, comportano anche un rischio di perdita (temporanea) di disponibilità dei dati. Se, per effettuare il restore (e/o per riparare il guasto), occorre molto tempo, per tutto questo tempo, il dato non è disponibile. Per mitigare questo rischio, entrano in gioco le tecniche di disaster recovery. In pratica, le tecniche di disaster recovery, effettuano delle copie, simili ai backup, ma tali da poter rendere disponibili i dati (ed i software di trattamento) in tempi molto brevi, anche in caso di indisponibilità del dispositivo originale. Molto spesso queste tecniche si basano sul principio di rendere disponibile, in Cloud o altro ambiente idoneo, una copia gemella del dispositivo che si è guastato, con tutto il suo contenuto in termini di software e dati. il tutto avviene in termini di decine di minuti, anziché di giorni.

6.2.10. Idoneo utilizzo del Cloud

Collocare dati in Cloud, in linea di principio, non pone rischi di sicurezza. I server dei primari fornitori Cloud, sono, tendenzialmente, molto più sicuri dei nostri server aziendali, perché vi sono decine di persone che, per lavoro, si occupano solo di sicurezza informatica. Il punto è sempre quello di utilizzare un fornitore affidabile, ed un servizio conforme al Regolamento. Tutti i principali fornitori Cloud offrono oggi questo genere di servizi. Un aspetto molto importante della conformità è quello di mantenere i dati all'interno dell'Unione Europea oppure in Paesi per i quali esiste una decisione di adeguatezza del Comitato o altre forme di garanzia riconosciute dal Regolamento (vedi 3.6. Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali). Naturalmente sono da considerare anche gli aspetti di sicurezza, backup, disaster recovery, cifratura dei dati, ecc. La prima cosa che sarebbe opportuno ottenere dal fornitore è la dichiarazione di rispondenza al Regolamento. Molto spesso è possibile scaricarla dal sito stesso, a volte "tagliata" sui servizi che stiamo utilizzando, e corredata di descrizione tecnica dei metodi utilizzati per garantire la conformità. È bene sottolineare che tutto ciò è presente nei servizi di tipo "business" (a pagamento), ma, in genere, non in quelli di tipo

“consumer” (gratis). Per questi ultimi, la conformità al Regolamento non viene garantita e, pertanto, sarebbe opportuno non mettervi dei dati personali.

Quasi tutti i servizi di memorizzazione su Cloud prevedono la cifratura dei dati all’origine, ovvero i dati vengono cifrati prima di partire dal nostro PC ed essere trasferiti al Cloud, e decifrati nel nostro PC dopo essere stati scaricati dal Cloud. Questa funzione garantisce la massima protezione dei dati ed andrebbe sempre attivata, in particolar modo, se il servizio Cloud viene utilizzato anche da dispositivi mobili, su reti WiFi che potrebbero non essere sicure. Se la cifratura/decifratura avviene sul dispositivo, è, ad oggi, impossibile intercettare i dati.

6.2.11. Profilazione utenti

La profilazione degli account degli utenti nei sistemi (file server, sistemi gestionali, applicativi web, ecc.) permette di limitare l’accesso ai dati personali solo al personale che necessita di lavorare su quei dati. Purtroppo non sempre i sistemi gestionali permettono una segmentazione degli accessi tale per cui effettivamente solo i dati necessari sono consultabili da ogni utente, tuttavia è in corso una forte evoluzione tecnologica a supporto della protezione dei dati personali.

La configurazione dei profili utente, anche e soprattutto in ambiente Windows (che è quello che solitamente rappresenta la prima porta di accesso ai documenti ed ai dati) non va solo definita correttamente “una tantum”, va anche aggiornata a fronte di variazioni che si verificano nell’organizzazione (assunzioni e dimissioni, cambiamenti di ruolo o mansione, interruzione dei rapporti di collaborazione).

7. SINTESI PER IL PROFESSIONISTA

7.1. Informazioni di base

Il 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 (regolamento generale sulla protezione dei dati) disciplina il trattamento dei dati personali nei Paesi appartenenti all'Unione Europea e si applica ai trattamenti di dati personali effettuati nella maggior parte degli ambiti, incluso quello lavorativo, ad esclusione di quelli che rientrano nell'esercizio di attività a carattere esclusivamente personale o domestico.

E' in vigore inoltre il DECRETO LEGISLATIVO 10 agosto 2018, n. 101, recante "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, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)" (in G.U. 4 settembre 2018 n.205), che ha l'obiettivo di aggiornare il Codice Privacy esistente e di coordinare la normativa italiana in materia di privacy con il Regolamento.

L'articolo 4 del Regolamento (vedi 3.1. Art.4: Definizioni) definisce come ***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".

Rientrano nella definizione di dati personali dunque i dati anagrafici, ma anche i dati di contatto personali o aziendali come l'indirizzo e-mail e numero di telefono, le immagini relative alla persona, dati relativi alla carta di credito e ai pagamenti, dati relativi alla situazione economica o patrimoniale, dati relativi all'attività lavorativa, dati relativi al grado di istruzione o di cultura o alla formazione ricevuta, e dati relativi all'utilizzo di sistemi informatici come l'indirizzo IP, MAC Address, marcatori temporanei (cookies) ecc.

Un approfondimento sulla natura dei dati personali corredato di esempi è disponibile al paragrafo 8.1. Dati personali, particolari categorie di dati personali e dati personali relativi a condanne penali e reati.

Analogamente il ***Trattamento di dati personali*** è "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".

Il ***Titolare del trattamento*** è "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali".

Un titolare del trattamento è ad esempio un professionista che tratta i dati personali dei propri clienti.

Il titolare del trattamento ha, tra le altre, la responsabilità di dimostrare, che il trattamento è effettuato conformemente al Regolamento (vedi 3.3.1.1. Art.5: Principi applicabili al trattamento di dati personali).

Il ***Responsabile del trattamento*** è "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento".

Un responsabile del trattamento è ad esempio un professionista del settore dell'informazione che gestisce l'infrastruttura informatica di un'azienda.

Il responsabile del trattamento ha, tra le altre, la responsabilità di agire in conformità con quanto disciplinato nel contratto o atto giuridico di designazione a responsabile e con le annesse istruzioni documentate del titolare del trattamento (vedi 3.5.1.3. Art.28,29: Responsabile del trattamento).

7.2. (In)formarsi e (in)formare

Il principio di responsabilizzazione (vedi 3.3.1.1. Art.5: Principi applicabili al trattamento di dati personali) lascia al titolare del trattamento l'onere di organizzare e dimostrare di aver adottato misure giuridiche, organizzative, tecniche adeguate a garantire la protezione dei dati personali: la mancanza di una "ricetta" per la conformità al Regolamento porta con sé la necessità di **formazione e aggiornamento costante per poter costruire e mantenere un sistema di gestione dei dati personali efficace**.

L'articolo 29 (vedi 3.5.1.3. Art.28,29: Responsabile del trattamento) e l'articolo 32 (vedi 3.8.1.1. Art.32: Misure di sicurezza tecniche e organizzative) del Regolamento recitano che "il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali, non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento".

Pertanto **l'istruzione del responsabile del trattamento sulle modalità di trattamento da adottare diventa un requisito obbligatorio come pure l'istruzione del personale che opera per conto del titolare**. L'istruzione si può concretizzare ad esempio in politiche e procedure di gestione dei dati personali per chiunque operi per conto del titolare ed in formazione per il personale dipendente.

7.3. Identificare i trattamenti svolti nell'attività lavorativa

Il primo passo per un'efficace protezione dei dati personali è **identificare i trattamenti dei dati personali stessi svolti durante l'attività lavorativa**.

Per identificare i trattamenti di dati personali può essere utile valutare in primis tutte le attività lavorative svolte e nell'ambito di tali attività individuare le operazioni di

raccolta/registrazione/conservazione, modifica, consultazione/comunicazione svolte su dati personali: ogni operazione costituisce o è parte di un trattamento di dati personali.

Infine occorre **distinguere se ogni trattamento è svolto in qualità di titolare o responsabile del trattamento**.

7.4. Raccogliere le informazioni sui trattamenti

Una volta individuati i trattamenti di dati personali svolti nell'attività lavorativa, occorre descriverli e corredarli di tutte le **informazioni** per mettere in atto e dimostrare di aver messo in atto un'efficace gestione dei dati personali stessi, tra cui quelle **utili a**:

1. **valutare l'adeguatezza delle misure di sicurezza adottate** in relazione al rischio sui trattamenti ed eventualmente adottare misure aggiuntive (vedi 7.5. Valutare l'adeguatezza delle misure di sicurezza e adottare misure di sicurezza aggiuntive);
2. **valutare se è necessaria una valutazione d'impatto** sulla protezione dei dati ed eventualmente eseguirla (vedi 7.6. Eseguire la valutazione d'impatto sulla protezione dei dati personali);
3. **redigere il registro delle attività di trattamento** (vedi 7.7. Redigere i registri delle attività di trattamento);
4. **designare i responsabili del trattamento** (vedi 7.8. Designare i responsabili del trattamento);
5. **redigere e distribuire le informative** (vedi 7.10. Redigere e distribuire le informative);
6. **raccogliere i consensi ai trattamenti e gestire le revoche** (vedi 7.11. Raccogliere il consenso ai trattamento e gestire eventuale revoca):
7. **organizzare i processi che trattano i dati personali** (vedi 7.12. Organizzare i processi che trattano i dati personali);
8. **gestire le violazione dei dati personali** (vedi 7.13. Gestire le violazione dei dati personali).

L'allegato 9.1. GDPR toolkit per i professionisti presenta un modello per la raccolta delle informazioni sui trattamenti e la generazione di documentazione utile ai punti sopra elencati.

7.5. Valutare l'adeguatezza delle misure di sicurezza e adottare misure di sicurezza aggiuntive

La **valutazione dell'adeguatezza delle misure di sicurezza adottate rispetto al rischio sui trattamenti di dati personali** è un punto chiave per una protezione efficace dei dati personali. Tuttavia la normativa non indica orientamenti specifici per l'individuazione del rischio connesso al trattamento, la sua valutazione in termini di origine, natura, probabilità e gravità, e l'individuazione di migliori prassi per attenuare il rischio: la scelte in materia di gestione del rischio sono responsabilità del titolare del trattamento, secondo il principio di responsabilizzazione.

Il paragrafo 4. VALUTAZIONE E GESTIONE DEI RISCHI PER I DIRITTI E LE LIBERTÀ DELLE PERSONE FISICHE espone un esempio di metodologia per la valutazione del rischio sui trattamenti ovvero per la valutazione dell'adeguatezza delle misure di sicurezza in atto.

In caso il titolare o responsabile del trattamento valuti come **necessario o desideri ridurre il rischio sui trattamenti,** può adottare **misure di sicurezza aggiuntive**, alcune delle quali sono descritte nel paragrafo 6. MISURE DI SICUREZZA A PROTEZIONE DEI DATI PERSONALI.

L'allegato 9.1. GDPR toolkit per i professionisti presenta un modello per la valutazione del rischio e la documentazione delle misure di sicurezza adottate e adottabili.

7.6. Eseguire la valutazione d'impatto sulla protezione dei dati personali

L'articolo 35 del Regolamento (vedi 3.8.1.2. Art.35,36: Valutazione d'impatto e consultazione preventiva) descrive come **necessaria, prima di procedere al trattamento, la valutazione d'impatto** qualora la valutazione del rischio evidenzi trattamenti ad alto rischio per i diritti e le libertà delle persone fisiche, ed In particolare in caso di:

- **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;
- **trattamento, su larga scala, di categorie particolari di dati personali** o di dati relativi a condanne penali e a reati; tuttavia il considerando 91 del Regolamento enuncia che *"il trattamento di dati personali* ***non dovrebbe essere considerato un trattamento su larga*** *scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato*" - e quindi per analogia **da parte di professionisti** in generale;
- la **sorveglianza sistematica su larga scala di una zona accessibile al pubblico**.

Ulteriori informazioni sulla valutazione d'impatto sono disponibili nel paragrafo 5. VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI.

7.7. Redigere i registri delle attività di trattamento

L'articolo 30 del Regolamento (vedi 3.7. Art.30: Registri delle attività di trattamento) recita che "ogni **titolare del trattamento** tiene un **registro delle attività** di trattamento svolte sotto la propria responsabilità**"** e analogamente **"**ogni **responsabile del trattamento** tiene un **registro** di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento".

Il registro delle attività di trattamento è un documento contenente le principali informazioni relative alle operazioni di trattamento svolte dal titolare e, se nominato, dal responsabile del trattamento; costituisce strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, indispensabile per ogni attività di valutazione o analisi del rischio.

Il Garante individua come **tenuti all'obbligo di redazione del registro**, tra gli altri, i **liberi professionisti con almeno un dipendente e/o che trattino dati sanitari e/o dati relativi a condanne penali o reati**, ma **ne raccomanda la redazione a tutti i titolari e responsabili del**

trattamento, in quanto strumento che contribuisce a meglio attuare il principio di responsabilizzazione e, al contempo, ad agevolare l'attività di controllo del Garante stesso.

Ulteriori informazioni sono disponibili nel paragrafo 3.7. Art.30: Registri delle attività di trattamento e nel paragrafo 3.7.2. Interpretazioni.

L'allegato 9.1. GDPR toolkit per i professionisti presenta un modello di registro delle attività di trattamento.

7.8. Designare i responsabili del trattamento

Quando un titolare affida ad un altro soggetto (generalmente un fornitore) un'attività di trattamento da svolgere "per proprio conto", quest'ultimo deve essere designato ***Responsabile del trattamento***.

È una figura prettamente esterna alla struttura del titolare, da non confondere con gli *Incaricati del trattamento*, la cui nomina era obbligatoria per il Codice Privacy Italiano.

L'*Articolo 28* del Regolamento (vedi 3.5.1.3. Art.28,29: Responsabile del trattamento) del Regolamento descrive la natura e gli oneri dei responsabili del trattamento.

I **responsabili del trattamento devono presentare garanzie sufficienti** per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento garantisca la tutela dei diritti dell'interessato: è responsabilità del titolare verificare tali requisiti.

I **trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico**, che vincoli il responsabile del trattamento al titolare del trattamento, **stipulato in forma scritta, anche in formato elettronico**.

Il titolare deve inoltre fornire al responsabile **istruzione documentata del titolare sulle modalità di trattamento, viceversa il responsabile deve** trattare i dati personali soltanto su **istruzione documentata del titolare del trattamento.**

Se il **responsabile del trattamento ricorre a un altro responsabile, deve essere data preventiva autorizzazione** scritta **del titolare del trattamento**. Quando un **responsabile del trattamento ricorre a un altro responsabile**, analogamente **su tale altro responsabile del trattamento sono imposti**, mediante un contratto o un altro atto giuridico, **gli stessi obblighi** in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento.

Ulteriori informazioni, compreso il contenuto dell'atto di designazione sono descritte nel paragrafo 3.5.1.3. Art.28,29: Responsabile del trattamento e paragrafo 3.5.2.3. Responsabile del trattamento.

7.9. Gestire i soggetti autorizzati al trattamento

Il ***Soggetto autorizzato al trattamento dei dati personali*** è la persona fisica che effettua materialmente le operazioni di trattamento sui dati personali sotto l'autorità diretta del titolare o del responsabile.

Risulta

- **consigliato**, sia per il titolare che per il responsabile, **designare i soggetti autorizzati al trattamento** dei dati personali che operano sotto la sua diretta autorità,
- consigliato,per il titolare, garantire che i soggetti autorizzati che operano sotto la sua diretta autorità siano impegnati alla riservatezza,
- **richiesto** dall' *Articolo 28* del Regolamento (vedi 3.5.1.3. Art.28,29: Responsabile del trattamento), **per il responsabile, garantire al titolare che le persone autorizzate al trattamento** dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato **obbligo legale di riservatezza**;
- **richiesto** dall' *Articolo 29* (vedi 3.5.1.3. Art.28,29: Responsabile del trattamento) e dall'*Articolo 32* (vedi 3.8.1.1. Art.32: Misure di sicurezza tecniche e organizzative) del Regolamento, sia per il responsabile sia per il titolare, che **ogni soggetto autorizzato al trattamento sotto la sua autorità non tratti i dati personali se non è istruito** in tal senso dal titolare del trattamento.

L'eventuale atto di designazione a soggetto incaricato al trattamento di dati personali non necessita di firma per accettazione, anche se è utile un' attestazione di presa visione, in particolare se l'atto è corredato delle istruzioni sul trattamento dei dati personali, a dimostrazione dell'impartizione delle istruzioni stesse.

Ulteriori informazioni sono disponibili nel paragrafo 3.5.2.4. Soggetti autorizzati al trattamento.

7.10. Redigere e distribuire le informative

I principi di trattamento corretto e trasparente implicano che l'interessato sia informato dell'esistenza del trattamento, delle sue finalità, e delle sue caratteristiche e modalità, tra cui l'esistenza di una profilazione e delle conseguenze della stessa, in caso di dati personali raccolti direttamente presso l'interessato, l'eventuale obbligo di fornire i dati personali e delle conseguenze in cui incorre se si rifiuta di fornirli, gli eventuali trasferimenti dei dati presso paesi extraeuropei, la base giuridica che rende leciti i trattamenti ed i trasferimenti extraeuropei, gli eventuali destinatari a cui saranno comunicati i dati.

Le informazioni fornite all'interessato relative al trattamento dei suoi dati personali sono comunemente definite ***Informativa sul trattamento dei dati personali***.

Le informazioni destinate al pubblico o all'interessato devono essere **concise, facilmente accessibili e di facile comprensione e che sia usato un linguaggio semplice** e chiaro.

L'interessato dovrebbe **ricevere le informazioni relative al trattamento di dati personali che lo riguardano al momento della raccolta** presso l'interessato o, se i dati sono ottenuti da altra fonte, entro un termine ragionevole, in funzione delle circostanze del caso.

In caso di attività professionale, l'informativa deve essere fornita nella maggior parte dei casi alle seguenti categorie di interessati

- **clienti e committenti**: normalmente un professionista tratta dati personali di persone fisiche che rappresentano clienti/committenti, ad esempio nome, cognome, telefono, e-mail, recapiti postali, ecc.;
- **fornitori**: quando questi sono persone fisiche, i dati relativi a persone giuridiche o società non sono da considerarsi come dati personali;

- **dipendenti e collaboratori**: i collaboratori possono ricadere nella categoria dei fornitori persone fisiche se prestano principalmente consulenze saltuarie, non continuative;
- **soggetti terzi**: come ad esempio Direttori dei Lavori, Progettisti di altre discipline, rappresentanti di Imprese appaltatrici, partner, ecc..

L'informativa ha di solito forma scritta e formato cartaceo o elettronico e può essere distribuita agli interessati tramite e-mail, può essere pubblicata sul sito web professionale, può essere allegata al contratto di fornitura, o consegnata a mano come documento cartaceo a se stante.

Sorge in molti casi la problematica di come dimostrare di aver fornito l'informativa all'interessato. Anche in questo caso il Regolamento non dà indicazioni precise ma lascia l'onere della prova al titolare.Può essere utile in tal senso conservare le e-mail inviate agli interessati, o in caso di informativa cartacea aggiungere una dicitura "ho letto e compreso" da corredare con la firma dell'interessato.

Ulteriori informazioni, anche in merito al contenuto dell'informativa, sono disponibili nei paragrafi 3.4.1.1. Art.12,13,14: Informazioni all'interessato relative al trattamento dei dati personali e 3.4.2.1. Informativa agli interessati.

L'allegato 9.1. GDPR toolkit per i professionisti presenta un riepilogo delle informazione sul trattamento da inserire nell'informativa.

7.11. Raccogliere il consenso ai trattamento e gestire eventuale revoca

Nei casi previsti dall'*Articolo 6* del Regolamento (vedi 3.3.1.2. Art.6: Liceità del trattamento), **è necessario richiedere all'interessato il consenso** per il trattamento dei dati personali quando il trattamento **non ha le seguenti basi giuridiche**:

- il trattamento è necessario **all'esecuzione di un contratto** di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- il trattamento è necessario per **adempiere un obbligo legale** al quale è soggetto il titolare del trattamento;
- il trattamento è necessario per la **salvaguardia degli interessi vitali** dell'interessato o di un'altra persona fisica;
- 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;
- il trattamento è necessario per il **perseguimento del legittimo interesse** del titolare del trattamento o di terzi;

oppure, nei casi previsti dall' *Articolo 9* del Regolamento (vedi 3.3.1.6. Art.9: Trattamento di categorie particolari di dati personali), ovvero **quando sono trattati particolari categorie di dati personali** e il trattamento non rientra nei seguenti casi:

- il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di **diritto del lavoro** e della sicurezza sociale e protezione sociale;

- il trattamento è necessario per **tutelare un interesse vitale dell'interessato** o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- il trattamento riguarda **dati personali resi manifestamente pubblici** dall'interessato;
- il trattamento è necessario per accertare, esercitare o difendere un **diritto in sede giudiziaria**;
- il trattamento è necessario per motivi di interesse pubblico;
- il trattamento è necessario per finalità di **medicina preventiva o di medicina del lavoro**, **valutazione della capacità lavorativa del dipendente**, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali; in questo caso i dati devono essere trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale.

Infine è necessario richiedere il consenso nei casi previsti dall' *Articolo 49* del Regolamento (vedi 3.6.1.5. Art.49: Deroghe in specifiche situazioni) ovvero in caso di **trasferimento dei dati personali verso un paese extra-europeo o un'organizzazione internazionale in mancanza di una decisione di adeguatezza e garanzie adeguate**.

Se contestualmente all'esecuzione di un contratto è previsto il trattamento di dati personali, è in ogni caso necessario richiedere il consenso per il trattamento dei dati personali non necessari all'esecuzione del contratto stesso.

In base alle definizioni (vedi 3.1. Art.4: Definizioni) il consenso è 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.

L'espressione del consenso deve essere libera. Non si può considerare libero, e quindi valido, un consenso espresso da un interessato che non ha reale scelta o che si sente costretto, che potrebbe procurare conseguenze negative se non dato, legato ad una parte non negoziabile di termini e condizioni di un contratto,che l'interessato non può revocare senza subire danno.

L'espressione del consenso deve essere specifica. Ovvero il consenso deve essere dato in relazione a una o più finalità specifiche.

L'espressione del consenso deve essere informata. Per ottenere un consenso valido, all'interessato dovrebbero essere fornite le opportune informazioni. Tali informazioni sono un sottoinsieme di quelle descritte nel paragrafo 3.4.1.1. Art.12,13,14: Informazioni all'interessato relative al trattamento dei dati personali, dette comunemente *informativa sul trattamento dei dati personali*.

Pertanto se si richiede il consenso contestualmente alla comunicazione della informativa, è sufficiente integrare le informazioni con quelle necessarie all'espressione del consenso.

La richiesta di consenso deve essere presentata in modo chiaramente distinguibile, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro.

Se il trattamento è basato sul consenso, il titolare del trattamento deve essere in grado di **dimostrare che l'interessato ha prestato il proprio consenso** al trattamento dei propri dati personali. Il titolare deve tenere conto di ciò nel scegliere la modalità di raccolta del consenso.

Il consenso potrebbe essere espresso mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Il consenso potrebbe dunque essere espresso attraverso la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto.

Non dovrebbe configurare consenso il silenzio, l'inattività o la preselezione di caselle.

L'interessato ha il diritto di **revocare il proprio consenso** in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Il consenso deve poter essere revocato con la stessa facilità con cui è accordato. Il titolare deve intraprendere a seguito della revoca del consenso tutte le azioni necessarie per interrompere o limitare i trattamenti di dati personali oggetto della revoca.

Ulteriori informazioni sulla raccolta e revoca del consenso sono disponibili nei paragrafi.

7.12. Organizzare i processi che trattano i dati personali

In base all'articolo 32 del Regolamento (vedi 3.8.1.1. Art.32: Misure di sicurezza tecniche e organizzative) il titolare, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, deve in atto misure tecniche e organizzative adeguate al livello di rischio sul trattamento stesso, quali se necessario la **pseudonimizzazione, la crittografia** e la **minimizzazione** dei dati trattati. Inoltre il titolare deve garantire che siano **trattati**, **per impostazione predefinita**, **solo i dati personali necessari** per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, **non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica**.

Inoltre, in base agli articoli dal 12 al 22 del Regolamento (vedi 3.4. Diritti dell'interessato), **il titolare del trattamento deve ottemperare alle richieste di esercizio dei diritti dell'interessato (**accesso, rettifica, cancellazione, limitazione del trattamento, notifica, portabilità dei dati, opposizione), se pertinenti, e fornire all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta al più tardi **entro un mese** dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste.

In ultimo l'articolo 33 del Regolamento (vedi 3.9.1.1. Art.33: Notifica di una violazione dei dati personali all'autorità di controllo) impone che il titolare del trattamento **documenti qualsiasi violazione dei dati personali**, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

Le disposizioni di cui sopra modificano significativamente i processi di gestione dei dati personali e i requisiti dei sistemi informatici a supporto dei trattamenti. In particolare il titolare dovrà a priori:

a) adottare processi o misure tecnologiche che, per trattamenti ad alto rischio, supportino **pseudonimizzazione, cifratura e minimizzazione dei dati**;

b) assicurarsi che siano **trattati solo i dati necessari alle finalità del trattamento**;
c) adottare un **sistema autorizzativo, informatico e non, tale per cui i dati personali siano accessibili solo ai soggetti autorizzati al trattamento**;
d) adottare processi e sistemi informatici che permettano di ottemperare alle **richieste di esercizio dei diritti dell'interessato** senza giustificato ritardo, entro un mese dalla richiesta o al massimo entro due mesi in caso di alta complessità di esercizio; in particolare processi e sistemi informatici devono garantire
    - il reperimento di tutti i dati personali relativi all'interessato,
    - l'esibizione dei dati personali dell'interessato senza divulgare di dati non pertinenti,
    - la rettifica i dati personali dell'interessato senza modificare informazioni non pertinenti,
    - la cancellazione o l'offuscamento dei dati personali dell'interessato senza danneggiare informazioni non pertinenti,
    - l'estrazione dei dati personali dell'interessato, trattati con mezzi automatizzati, in un formato strutturato, di uso comune e leggibile da dispositivo automatico al fine di trasmettere tali dati a un altro titolare**,** senza divulgare di dati non pertinenti;
e) adottare processi e sistemi informatici che permettano di rilevare e documentare le eventuali **violazioni di dati personali**.

A titolo di esempio misure a supporto di quanto sopra possono essere la riorganizzazione di archivi cartacei ed elettronici, l'adozione di software di ricerca e indicizzazione per i dati non strutturati, l'adozione di software gestionali specifici, strumenti per il monitoraggio e la segnalazione delle intrusioni nelle reti e nei sistemi informatici del titolare. In particolare si stanno diffondendo soluzione tecnologiche «GDPR ready», ovvero servizi e prodotti informatici i cui produttori in fase di sviluppo e progettazione hanno tenuto conto delle disposizioni del Regolamento per far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi.

7.13. Gestire le violazione dei dati personali

Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

In base all'articolo 33 del Regolamento (vedi 3.9.1.1. Art.33: Notifica di una violazione dei dati personali all'autorità di controllo), non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il **titolare del trattamento dovrebbe notificare la violazione dei dati personali al Garante**, senza ingiustificato ritardo e, ove possibile, **entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche**.

Ad esempio la segnalazione al Garante può essere effettuata attraverso la compilazione del modulo disponibile al seguente link (attenzione, è richiesto l'utilizzo della firma digitale):

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1915835

e la trasmissione del modulo compilato al Garante attraverso posta elettronica certificata all'indirizzo protocollo@pec.gpdp.it

In base all'articolo 34 del Regolamento (vedi 3.9.1.2. Art.34: Comunicazione di una violazione dei dati personali all'interessato), il **titolare del trattamento dovrebbe comunicare anche all'interessato la violazione dei dati personali** senza indebito ritardo, qualora questa violazione dei dati personali sia suscettibile di **presentare un rischio elevato per i diritti e le libertà della persona fisica**, al fine di consentirgli di prendere le precauzioni necessarie.

8. APPROFONDIMENTI

8.1. Dati personali, particolari categorie di dati personali e dati personali relativi a condanne penali e reati

L'articolo 4 del Regolamento (vedi 3.1. Art.4: Definizioni) definisce il dato personale come "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".

I dati personali possono anche

- appartenere a particolari categorie di dati personali ovvero rivelare 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,
- oppure essere relativi a condanne penali e reati.

Esempi di dati personali che non appartengono a particolari categorie di dati personali e non sono relativi a condanne penali e reati risultano:

- dati anagrafici - nome, cognome, data e luogo di nascita, età, genere, cittadinanza, lingua, luogo di residenza, codice fiscale, stato civile, stato matrimoniale, stato di famiglia, rapporti di parentela, ecc.;
- immagini relative alla persona - foto, audio e video;
- dati relativi a documenti identificativi - carta d'identità, patente, passaporto, ecc.
- dati relativi alla carta di credito e ai pagamenti, abitudini/interessi/preferenze personali di consumo, prodotti o servizi acquistati,
- dati relativi all'ubicazione o posizione geografica,
- dati relativi alla situazione economica o patrimoniale,
- dati relativi provvedimenti o procedimenti sanzionatori, disciplinari, amministrativi o contabili;
- dati di contatto personali e aziendali - indirizzo e-mail e PEC, numero di telefono fisso/cellulare/fax, identificativo nei sistemi di messaggistica (Skype, Telegram, ecc.), ecc.;
- dati relativi all'attività lavorativa - azienda di appartenenza, dati contrattuali (posizione, inquadramento, data di assunzione, matricola, ecc.), dati di presenza in azienda (accessi fisici, orari di ingresso/uscita, permessi non idonei ad indicare lo stato di salute, ferie, ecc.), dati relativi alle trasferte (dati di viaggio, rimborsi spese, multe e contravvenzioni, ecc.), dati relativi alla retribuzione, comprese le trattenute (IBAN di accredito, bonus, premi di produzione, cessione quinto stipendio, finanziamenti, ecc.) , valutazione della prestazione lavorativa, ecc.;
- dati relativi al grado di istruzione o di cultura o alla formazione ricevuta,

- dati relativi all'utilizzo di sistemi informatici - log-in/ log-out, ricerche in rete, indirizzo IP, MAC Address, cronologia di navigazione web, username, marcatori temporanei (cookies) o a identificativi di altro tipo, come i tag di identificazione a radiofrequenza ecc.

Esempi di dati che appartengono a *particolari categorie di dati personali* risultano:

- dati che rivelino l'origine razziale o etnica - permessi e carte di soggiorno;
- dati che rivelino le opinioni politiche;
- dati che rivelino le convinzioni religiose;
- dati che rivelino le convinzioni filosofiche;
- dati che rivelino l'appartenenza sindacale - permessi e congedi sindacali, trattenute sindacali o opinioni sindacali;
- dati genetici o biometrici volti a identificare in modo univoco una persona fisica - impronte digitali, dati relativi a iride e retina, dati fisiognomici idonei al riconoscimento facciale, andatura, movimento delle labbra, digitazione su tastiera, Rilevazione facciale attraverso uno o più elementi, ecc.;
- dati idonei a rivelare lo stato di salute, fisico o mentale, presente o futuro - un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari; le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, dati idonei a rivelare malattie infettive e diffusive (HIV, ecc.), certificazioni sanitarie attestanti lo stato di malattia, assenza dal lavoro per malattia, giustificativi visite mediche, dati relativi a sinistri e infortuni, dati relativi a a invalidità, infermità, o disabilità, utilizzo di particolari ausili protesici, l'appartenenza a categorie protette, dati riferiti a gravidanza, puerperio o allattamento, giudizi di idoneità e limitazione alla mansione, dati relativi all'assunzione di droghe e/o alcol, preferenze/abitudini alimentari idonee a rivelare lo stato di salute (allergie, celiachia, ecc.);
- dati relativi al collocamento obbligatorio;
- dati idonei a rivelare la vita sessuale e l'orientamento sessuale della persona;
- trattenute e pignoramenti della retribuzione;
- dati da cui sono desumibili altri dati che rientrano nelle categorie precedenti (curriculum vitae, navigazione internet, acquisto prodotti e servizi, ecc.).

Per *dati relativi a condanne penali e reati* si intendono tutti i dati che hanno rilevanza nell'area penale, in particolare quelli menzionati dal casellario giudiziario di ciascun individuo, quel schedario istituito presso la Procura presso ogni tribunale penale ordinario della Repubblica italiana, con lo scopo di raccogliere e conservare gli estratti dei provvedimenti dell'autorità giudiziaria, in modo tale che sia sempre possibile conoscere l'elenco dei precedenti penali di ogni cittadino. I dati giudiziari sono dunque quelli inerenti alla sussistenza di carichi pendenti e condanne penali.

Nel primo caso sono quei dati capaci di indicare l'esistenza di procedimenti penali in corso e non definiti, nel secondo le eventuali pene con cui il cittadino è stato sanzionato per la condotte in ordine alle quali è stato riconosciuto responsabile di reato: per esempio la condizione di indagato od imputato in un giudizio penale per la contestazione di una condotta penalmente rilevante, oppure in caso di condanna già avvenuta, la pena con cui la sentenza o il decreto penale irrevocabile all'esito di un giudizio ha giudicato la sussistenza di un reato, (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di

soggiorno, le misure alternative alla detenzione), oppure una misura di sicurezza (arresto, fermo) oppure ancora un decreto di espulsione di un cittadino straniero.

Esempi di dati personali *relativi a condanne penali e reati* risultano:

- certificato dei carichi pendenti,
- casellario giudiziale,
- dati relativi a provvedimenti e cause giudiziarie,
- documentazione afferente a contenziosi penali,
- comunicazione di iscrizione indagato,
- dati relativi ad eventuali controversie con precedenti datori di lavoro.

8.2. Trattamento di dati personali nel ruolo di CTU e CTP

Nel caso di incarico conferito per assolvere il ruolo di CTU o di Consulente Tecnico di Parte, CTP occorre prendere in esame, quale unico riferimento normativo esistente,le “Linee guida in materia di trattamento di dati personali da parte dei consulenti tecnici e dei periti ausiliari del giudice e del pubblico ministero”, provvedimento risalente e pubblicato nella Gazzetta Ufficiale, (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1534086), n. 178 del 31 luglio 2008.

Le linee guida del Garante per CTU e CTP, chiariscono intanto che i dati giudiziari e sensibili trattati da coloro che ricoprono il ruolo di ausiliario del giudice o di consulente privato, sono conosciuti per “ragioni di giustizia” come riportava l’art 47 del Codice della Privacy, ora abrogato dal D.Lgs 101/2018 che disciplina l’argomento all’Art. 2-octies “Principi relativi al trattamento di dati relativi a condanne penali e reati”, fatto salvo quanto disposto dal D. Lgs 51/2018.

Ciò premesso, occorre distinguere tra esoneri dagli obblighi normalmente previsti e gli obblighi cui continuano a soggiacere i professionisti nominati CTU o CTP.

Questi ultimi **non sono tenuti** a seguire le norme che disciplinano:

- modalità di esercizio dei diritti da parte dell'interessato;
- al riscontro da fornire al medesimo;
- i codici di deontologia e di buona condotta;
- l'informativa agli interessati;
- la cessazione del trattamento;
- il trattamento svolto da soggetti pubblici;
- obblighi di comunicazione all´Autorità;
- autorizzazioni e al trasferimento dei dati all´estero e ricorsi al Garante

Restano a loro carico i seguenti obblighi:

- princìpi di liceità, finalità, correttezza, pertinenza, nonchè oggi pare opportuno ritenere valido anche il rispetto del principio di *accountability*;
- adottare le misure di sicurezza idonee a preservare i dati da alcuni eventi, tra i quali accessi e utilizzazioni indebite

Queste appaiono le regole che governano l’attività dei CTU:

- Limitarsi nel proprio incarico ad utilizzare i soli dati necessari all'espletamento dello stesso;
- Comunicare i dati alle sole parti coinvolte e all'Autorità Giudiziaria che ha effettuato la nomina;
- salvo quanto eventualmente stabilito da puntuali disposizioni normative o da specifiche autorizzazioni dell´autorità giudiziaria che dispongano legittimamente ed espressamente in senso contrario, il consulente e il perito non possono conservare, in originale o in copia, in formato elettronico o su supporto cartaceo, informazioni personali acquisite nel corso dell´incarico concernenti i soggetti, persone fisiche o giuridiche, nei cui confronti hanno svolto accertamenti, nemmeno in caso di rinuncia o revoca dell'incarico;
- l'espletamento di eventuali ulteriori attività dell´ausiliare, conseguenti a richieste di chiarimenti o di supplementi di indagine, il consulente e il perito possono soddisfarle acquisendo dal fascicolo processuale, in conformità alle regole poste dai codici di rito, la documentazione necessaria per fornire i nuovi riscontri;
- Assumersi la responsabilità durante tutta la durata dell'incarico, sino dunque all'esito dell'elaborato peritale, adottando le misure tecniche adeguate a tutelare i dati in sua custodia.

Invece, il CTP consulente di parte:

- può trattare lecitamente i dati personali nei limiti in cui ciò è necessario per il corretto adempimento dell'incarico ricevuto dalla parte o dal suo difensore ai fini dello svolgimento delle indagini difensive di cui alla legge n. 397/2000 o, comunque, per far valere o difendere un diritto in sede giudiziaria, dati sensibili o giudiziari possono essere utilizzati solo se ciò è indispensabile;
- può acquisire e utilizzare solo i dati personali comunque pertinenti e non eccedenti rispetto alle finalità perseguite con l'incarico ricevuto, avvalendosi di informazioni personali e di modalità di trattamento proporzionate allo scopo perseguito;
- salvi i divieti di legge posti a tutela della segretezza e riservatezza delle informazioni acquisite nel corso di un procedimento giudiziario (cfr., ad esempio, l´art. 379-bis c.p.p.) e i limiti e i doveri derivanti dal segreto professionale e dal fedele espletamento dell'incarico ricevuto (cfr. artt. 380 e 381 c.p.), può comunicare a terzi dati personali solo ove ciò risulti necessario per finalità di tutela dell´assistito, limitatamente ai dati strettamente funzionali all´esercizio del diritto di difesa della parte e nel rispetto dei diritti e della dignità dell'interessato e di terzi;
- relativamente ai dati personali acquisiti e trattati nell´espletamento dell´incarico ricevuto da una parte, assume personalmente le responsabilità e gli obblighi relativi al profilo della sicurezza prescritti dal Regolamento e ove l´incarico comporti il trattamento con strumenti elettronici di dati sensibili o giudiziari, in passato era tenuto a redigere il documento programmatico sulla sicurezza (art. 33, comma 1, lett. g) e punto 19. del disciplinare tecnico allegato B), dunque oggi potrebbe essere ritenuto opportuno tenere il Registro dei Trattamenti, secondo quanto prescrive il Regolamento;
- deve nominare per iscritto gli eventuali collaboratori, anche se adibiti a mansioni di carattere amministrativo, quali che siano addetti alla custodia e al trattamento, in qualsiasi forma, dei dati personali impartendo loro precise istruzioni sulle modalità, ambito del trattamento loro consentito e sulla scrupolosa osservanza della riservatezza dei dati di cui vengono a conoscenza.

8.3. Principio di responsabilizzazione o “accountability”

Le legislazioni precedenti imponevano determinate e dettagliate misure di sicurezza a protezione dei dati personali (vedi *Allegato B del Codice Privacy*) e determinati rimedi alle possibili violazioni e conseguenti danni. Tale approccio si è dimostrato fallimentare nel garantire una reale e sostanziale difesa per i diritti e le libertà delle persone fisiche, perchè limitativo e non adeguato a sostenere l’evoluzione tecnologica dei sistemi e conseguentemente delle minacce ad essi associate.

L’entrata in vigore del Regolamento ha, di fatto, modificato radicalmente l’approccio adottato finora per la regolamentazione della materia, introducendo il principio di responsabilizzazione o “accountability”.

Il principio era stato già preso in considerazione nel 2010 dal Gruppo di Lavoro Articolo 29, nell’ “Opinion 3/2010 on the principle of accountability”, che raccomanda che “il titolare del trattamento dei dati debba essere in grado di dimostrare di avere adottato un processo complessivo di misure giuridiche, organizzative, tecniche, per la protezione dei dati personali, anche attraverso l’elaborazione di specifici modelli organizzativi e che debba dimostrare in modo positivo e proattivo che i trattamenti di dati effettuati sono adeguati e conformi al regolamento europeo in materia di privacy”.

Il principio di responsabilizzazione permea tutto il Regolamento, e si traduce in particolare negli articoli 32 e 35 (vedi 4.8. Protezione dei dati e valutazione del rischio) che recitano “ ...il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio” e “quando un tipo di 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”**.**

Secondo questo nuovo approccio **il titolare avrà discrezionalità e libertà nella scelta della modalità di tutela dei dati adeguate, secondo una sua valutazione soggettiva**, alle tecnologie utilizzate e alla natura, all'oggetto, al contesto e alle finalità del trattamento.

Se da un lato questo approccio appare destinato a garantire una maggior protezione dei dati personali, esso comporta l’onere del titolare di dimostrare l’adeguatezza delle soluzioni adottate e i conseguenti rischi derivanti dal fatto che le sue valutazioni soggettive sull’adeguatezza delle modalità di tutela possono discordare da quelle dell’autorità di controllo.

8.4. I diritti dell’interessato

Il Regolamento ha rivoluzionato il concetto del dato rispetto al passato.

Oggi il Regolamento Europeo considera il dato come un qualsiasi *“bene”*, essendo divenuto suscettibile di valore economico, ma soprattutto perchè come tutti i beni, appartiene a qualcuno e dunque hanno un soggetto *“proprietario”* che è denominato dalle norme in materia *interessato*.

L’interessato essendo dunque proprietario di tutti i dati che gli afferiscono detiene anche il riconoscimento di non pochi diritti.

I diritti di cui gode sono aumentati anche a fronte dell'ingresso nel panorama normativo di diritti per così dire, prima privi di una propria affermazione, come per esempio il diritto all'oblio, quale strumento di tutela dell'identità personale.

L'interessato può dunque esercitare una serie di diritti, alcuni consolidati dalla precedente disciplina, altri del tutto nuovi, come la portabilità.

I diritti, "vecchi" e nuovi, che l'interessato ha titolo ad esercitare sono i seguenti:

- informazioni, comunicazioni e modalità di trasparenza per l'esercizio dei diritti dell'interessato (articolo 12 del Regolamento, vedi 3.4.1.10. Art.12: Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato);
- diritto di accesso (articolo 15 del Regolamento, vedi 3.4.1.2. Art.15: Diritto di Accesso),
- diritto di rettifica (articolo 16 del Regolamento, vedi 3.4.1.3. Art.16: Diritto di rettifica),
- diritto alla cancellazione (c.d. "Diritto all'oblio") (articolo 17 del Regolamento, vedi 3.4.1.4. Art.17: Diritto alla cancellazione («diritto all'oblio»)),
- diritto di limitazione di trattamento (articolo 18 del Regolamento, vedi 3.4.1.5. Art.18: Diritto di limitazione di trattamento),
- diritto a che il Titolare notifichi la rettifica o la cancellazione ai destinatari (articolo 19 del Regolamento, vedi 3.4.1.6. Art.19: Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento),
- diritto alla Portabilità dei dati (articolo 20 del Regolamento, vedi 3.4.1.7. Art.20: Diritto alla portabilità dei dati),
- diritto di opposizione (articolo 21 del Regolamento, vedi 3.4.1.8. Art.21: Diritto di opposizione).

A questi occorre poi aggiungere anche il diritto di revoca di cui all'articolo 7 del Regolamento (vedi 3.3.1.4. Art.7: Condizioni per il consenso), istituto che ha trovato una sua puntuale definizione e disciplina.

E' indubitabile come a ciascuno di questi diritti debba essere "concepita" ed ideata una vera e propria procedura che soddisfi, nella logica del principio di accountability, il principio di privacy by design mediante la pianificazione di processi descriva le modalità che il Titolare ha previsto per consentire all'interessato l'esercizio di ogni diritto che gli sia proprio, senza improvvisare.

Essenzialmente occorre distinguere uno spartiacque fra i diritti in capo all'interessato fra **diritti conoscitivi** e **diritti di controllo** inerenti ai propri dati.

Il **diritto all'informativa,** di cui all'articolo 12 del Regolamento, è certamente quel diritto che, non solo sancisce il valore del dato di una persona riconoscendone la pretesa legittima di conoscere preventivamente quali sono le ragioni, gli scopi, i destinatari, il Titolare della richiesta che viene avanzata dei propri dati, ma soprattutto perché su questo diritto si fonda gran parte della liceità dei trattamenti, tanto da poterlo definire senza alcuna incertezza la "chiave di volta" dell'architettura delle tutele a vantaggio dell'interessato e della stessa disciplina in materia di protezione dei diritti personali.

Anche il **diritto d'accesso** è un diritto di tipo conoscitivo perché è il mezzo con cui l'interessato ha diritto di richiedere ed ottenere informazioni durante il trattamento circa:

- le finalità trattamento;
- le categorie dei dati personali trattati;
- i destinatari o le categorie di destinatari a cui i dati sono o saranno comunicati;

- il periodo di conservazione dei dati se previsto;
- criteri di conservazione dei dati;
- il diritto di proporre reclamo;
- se i dati non sono trattati presso il titolare indicazioni circa la loro origine;
- le garanzie adeguate e predisposte in caso di trasferimento dei dati a un paese terzo e/o organizzazione internazionale.

Laddove l'interessato richiedesse le informazioni sopra elencate, il Titolare del trattamento ai sensi dell'articolo 15 del Regolamento è tenuto a:

- attivarsi e soddisfare gratuitamente la richiesta ricevuta, fornendo all'interessato una copia dei dati personali trattati, senza pretendere che quest'ultimo fornisca particolari motivazioni (entro un mese dal ricevimento della richiesta, prorogabile di due mesi tenuto conto del numero e/o della complessità delle richieste ulteriori eventualmente ricevute, previo avviso all'interessato);
- addebitare all'interessato solo se richiedesse l'inoltro di più copie, una somma forfettaria commisurata ai costi amministrativi standard sostenuti;
- rifiutarsi di rilasciare le informazioni richieste se non è in grado di identificare l'interessato;
- potrà fornire le informazioni richieste dall'interessato per iscritto e/o con l'ausilio di mezzi elettronici, ed in quest'ultimo caso avvalersi di un formato elettronico di uso comune (per esempio: .doc; .pdf; .xml; xls; .ods etc);
- nel caso non riesca ad adempiere alla richiesta ricevuta, dovrà informare senza ritardo e comunque entro un mese l'interessato sui relativi motivi ostativi e della possibilità per lo stesso di proporre reclamo ad una autorità di controllo o un ricorso giurisdizionale;
- attestare di avere adempiuto alla richiesta richiesta ricevuta mediante comunicazione scritta
- all'interessato o anche oralmente previa richiesta dello stesso a procedere in tal senso, e previo accertamento della sua identità.

Se la richiesta e/o le richieste dell'interessato eventualmente ricevute dovessero risultare manifestamente infondata/e o eccessive, il Titolare può:

- addebitare un contributo spese tenuto conto dei costi amministrativi sostenuti per soddisfare la/le richiesta/e;
- rifiutare di darvi corso a patto che ne dimostri la manifesta infondatezza e/o eccessività.

Tra i *diritti di controllo*, che prevedono la possibilità per l'avente diritto di essere parte attiva ed intervenire richiedendo di modificare i dati o il trattamento sin qui effettuato, il primo è senza dubbio il **diritto di rettifica**.

In caso di presentazione da parte dell'interessato di tale richiesta, il Titolare del trattamento ai sensi dell'articolo 16 del Regolamento è tenuto a:

- attivarsi tempestivamente e senza ingiustificato ritardo (entro un mese dal ricevimento della richiesta prorogabile di due mesi tenuto conto del numero e/o della complessità delle richieste ulteriori eventualmente ricevute, previo avviso all'interessato) procedendo alla rettifica dei predetti dati ovvero a dar corso all'attività di integrazione e/o aggiornamento e/o integrazione dei dati, su qualsiasi supporto sia esso cartaceo o elettronico in cui gli stessi risultino contenuti e custoditi;

- rifiutarsi di rilasciare le informazioni richieste se non è in grado di identificare l'interessato;
- comunicare le modifiche e/o integrazioni e/o aggiornamenti apportati anche agli altri soggetti eventualmente coinvolti nel trattamento dei dati (per esempio responsabile e/o responsabili del trattamento, eventuali incaricati se nominati, soggetti terzi a cui i dati siano stati comunque comunicati e/o diffusi);
- dovrà attestare di avere proceduto a quanto richiesto mediante comunicazione scritta all'interessato o anche oralmente previa richiesta dello stesso e a patto che la sua identità venga accertata;
- nel caso in cui non riesca ad adempiere alla richiesta ricevuta, dovrà informare senza ritardo e comunque entro un mese l'interessato sui relativi motivi ostativi e della possibilità per lo stesso di proporre reclamo ad una autorità di controllo o un ricorso giurisdizionale.

Se la richiesta e/o le richieste dell'Interessato eventualmente ricevute dovessero risultare manifestamente infondata/e o eccessive il Titolare può:

- addebitare un contributo spese tenuto conto dei costi amministrativi sostenuti per soddisfare la/le richiesta/e;
- rifiutare di darvi corso a patto che ne dimostri la manifesta infondatezza e/o eccessività.

In virtù del Regolamento l'interessato vede finalmente riconosciuto per la prima volta in modo esplicito il diritto all'oblio, la possibilità di "essere dimenticato" e dunque di ottenere **il diritto alla cancellazione** dei dati personali che lo riguardano nei seguenti casi:

- i dati personali non sono più necessari rispetto alle finalità indicate nel trattamento e per le quali è avvenuta la raccolta;
- revoca del consenso su cui si basa il trattamento se non esiste altro motivo legittimante il trattamento stesso;
- opposizione al trattamento in assenza di motivi legittimanti comunque il trattamento stesso;
- opposizione al trattamento per finalità di marketing diretto;
- trattamento illecito dei dati;
- la cancellazione dei dati risulta necessaria per adempiere ad obblighi legali previsti dal diritto dell'Unione Europea o dello stato membro cui è soggetto il Titolare;
- la raccolta dei dati è avvenuta relativamente ad una offerta di servizi delle società di informazione.

In caso di presentazione da parte dell'interessato di tale richiesta, il titolare del trattamento ai sensi dell'articolo 17 del Regolamento sarà tenuto a:

- attivarsi obbligatoriamente e senza ingiustificato ritardo (ovvero entro un mese dal ricevimento della richiesta prorogabile di due mesi tenuto conto del numero e/o della complessità delle richieste ulteriori eventualmente ricevute, previo avviso all'interessato) procedendo alla cancellazione dei predetti dati su ciascuno strumento sia esso rappresentato da un supporto cartaceo od elettronico in cui gli stessi risultino essere stati sino ad ora contenuti ed archiviati;
- rifiutarsi di rilasciare le informazioni richieste se non è in grado di identificare l'interessato;
- se i dati personali sono stati resi pubblici, dovrà comunicare l'intervenuta elaborazione della richiesta di cancellazione dei dati agli altri soggetti coinvolti nel trattamento dei dati

(per esempio responsabile e/o eventuali responsabili del trattamento, eventuali incaricati se nominati, soggetti terzi a cui i dati siano stati comunque comunicati o diffusi) affinché questi possano procedere a loro volta alla cancellazione di qualsiasi *link*, copia o riproduzione dei predetti dati;
- attestare di avere proceduto alla cancellazione dei dati mediante comunicazione scritta all'interessato o anche oralmente previa richiesta dello stesso ed accertamento della sua identità;
- nel caso non riesca ad adempiere alla richiesta ricevuta, informare senza ritardo e comunque entro un mese l'interessato sui relativi motivi ostativi e della possibilità per lo stesso di proporre reclamo ad una autorità di controllo o un ricorso giurisdizionale;

Il Titolare non sarà tenuto a soddisfare la richiesta laddove il trattamento:

1. il trattamento sia necessario per l'esercizio del diritto alla libertà di espressione ed informazione (per es.: il diritto di cronaca);
2. sussista un obbligo legale;
3. vi siano motivi di pubblico interesse nel settore della sanità pubblica;
4. sia necessaria l'archiviazione nel pubblico interesse di ricerca scientifica o storica o a fini statistici;
5. accertamento, esercizio o la difesa di un diritto in sede giudiziaria.

Esiste poi **il diritto di limitazione**, quello che concede la possibilità all'interessato di assicurarsi che i suoi dati siano utilizzati limitatamente a quanto necessario ai fini della conservazione.

La limitazione può essere definita e intesa, anche nella prassi, come "il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro" (articolo 4 Regolamento, vedi 3.1. Art.4: Definizioni).

Questa definizione dovrà essere considerata soprattutto da chi si occupa di programmazione e sviluppo dei sistemi informativi: sarà necessario prevedere una modalità che permetta di "contrassegnare" i dati personali memorizzati, i quali possono essere *limitati* in qualunque momento da parte dell'interessato o del Garante. Potrebbe essere interpretata anche come una sospensione temporanea (capace anche di divenire permanente) del trattamento in corso: unica eccezione è la conservazione dei dati, che, peraltro, può essere adottata dal Titolare solo dopo la valutazione di una serie di circostanze.

In particolare tale facoltà è esercitabile laddove:

- l'interessato contesti l'esattezza dei dati personali forniti affinché ne sia verificata l'effettiva correttezza;
- l'interessato in presenza di un trattamento illecito dei suoi dei dati non proceda chiedendone la cancellazione;
- il trattamento dei dati risulti necessario non per le finalità del trattamento ma per l'esercizio del diritto di difesa o di altro diritto in sede giudiziaria;
- l'interessato si sia opposto al trattamento dei dati e siano ancora in corso le verifiche per accertare la prevalenza o meno dei motivi legittimanti il trattamento da parte del titolare sui diritti dell'interessato.

In tal caso il Titolare del trattamento ai sensi dell'articolo 18 del Regolamento:

- dovrà attivarsi obbligatoriamente nelle ipotesi sopra descritte (entro un mese dal ricevimento della richiesta prorogabile di due mesi tenuto conto del numero e/o della

complessità delle richieste ulteriori eventualmente ricevute, previo avviso all'interessato) avvalendosi di un sistema automatizzato o di altra modalità (per esempio predisposizione di un elenco in formato elettronico o cartaceo contenente tali dati, a fianco dei quali dovrà essere dato atto della limitazione di trattamento a cui gli stessi dovranno d'ora in avanti essere assoggettati) per ottenere l'inaccessibilità dei dati;

- potrà rifiutarsi di rilasciare le informazioni richieste se non è in grado di identificare l'interessato;
- dovrà informare anche gli altri soggetti coinvolti nel trattamento dei predetti dati (per esempio responsabile e/o eventuali responsabili del trattamento, eventuali incaricati se nominati, soggetti terzi a cui i dati siano stati comunque comunicati o diffusi);
- impedire e bloccare ulteriori operazioni di trattamento sui dati ad eccezione della loro semplice conservazione;
- attestare di avere proceduto alla limitazione delle operazioni di trattamento dei dati mediante comunicazione scritta all'interessato o anche oralmente previa richiesta dello stesso ed accertamento della sua identità;
- potrà sbloccare i dati precedentemente limitati soltanto previo consenso espresso in tal senso da parte dell'interessato (oppure i dati potranno essere comunque trattati laddove sia necessario l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di rilevante interesse pubblico in base a una norma dell'Unione o dell'ordinamento interno);
- informare l'interessato di avere proceduto alla limitazione prima che la stessa sia eventualmente revocata;
- nel caso non riesca ad adempiere alla richiesta ricevuta, dovrà informare senza ritardo e comunque entro un mese l'interessato sui relativi motivi ostativi e della possibilità per lo stesso di proporre reclamo ad una autorità di controllo o un ricorso giurisdizionale.

Un altro diritto nel novero del controllo da parte dell'interessato dei propri dati e la libertà di scegliere *come* e se farli circolare, costituiscono i traguardi raggiunti per la Protezione dei Dati dal Regolamento.

In particolare, il **diritto alla portabilità** del dato consente all'interessato di ricevere i dati personali forniti ad un titolare in "un formato strutturato, di uso comune e leggibile da un dispositivo automatico e di trasmetterli ad un titolare diverso senza impedimenti" ed eventualmente di riutilizzarli per altri scopi. È prevista poi la possibilità che i dati personali siano trasmessi direttamente da un Titolare all'altro su richiesta espressa dell'interessato.

Viceversa, tutti i dati personali che siano creati dal titolare nell'ambito di un trattamento, per esempio attraverso procedure di personalizzazione o finalizzate alla formulazione di raccomandazioni, o attraverso la categorizzazione o profilazione degli utenti, sono dati derivati o dedotti dai dati personali forniti dall'interessato e non ricadono nell'ambito del diritto alla portabilità.

I dati possono essere così suddivisi:

- dati forniti consapevolmente e attivamente dall'interessato: indirizzo postale, nome utente, età, ecc.;
- dati osservati forniti dall'interessato attraverso la fruizione di un servizio o l'utilizzo di un dispositivo: la cronologia delle ricerche effettuate dall'interessato, dati relativi al traffico, dati relativi all'ubicazione nonché altri dati grezzi come la frequenza cardiaca registrata da dispositivi sanitari o di fitness.

In particolare tale facoltà è esercitabile laddove:

- il trattamento si basa sul consenso dell'interessato (sempre che il trattamento sia "effettuato con mezzi automatizzati" e non attraverso archivi o registri cartacei).
- su un contratto di cui è parte l'interessato.

Il Titolare di fronte ad una tale richiesta non potrà essere impreparato in quanto sarà tenuto a garantire ai sensi dell'articolo 20 del Regolamento:

- l'adempimento degli obblighi informativi,
- la valutazione dei rischi specifici della portabilità,
- l'adozione di misure tecniche e/o organizzative adeguate a garantire il suddetto diritto dell'interessato.

Infine è stato riaffermato il **diritto** che l'interessato ha **di opporsi** in qualsiasi momento, per la propria posizione personale, al trattamento dei dati personali che lo riguardano inerente a ragioni di interesse pubblico o all'esercizio di pubblici poteri (ai sensi dell'*Articolo 6*, paragrafo 1, lettera e) del Regolamento). Tale diritto trova la sua giustificazione nella tutela che ciascun individuo può mettere in atto di fronte al controllo eccessivo dello Stato. L'interessato può opporsi anche al trattamento posto in essere per il perseguimento di legittimi interessi del titolare o di terzi (art. 6, par. 1, lett. f), compresa la profilazione sulla base di tali disposizioni.

Il Titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

L'interessato può opporsi anche al trattamento dei dati per fini commerciali, come marketing diretto e profilazione. Occorre tenere presente che l'opposizione al trattamento è operazione diversa dalla cancellazione dei dati. In base ad essa l'interessato può impedire il trattamento che non è compatibile con le finalità del consenso. Il Titolare del trattamento è tenuto a dare riscontro alla richiesta dell'interessato secondo questi modalità:

1. *termini*: entro 1 mese dall'esercizio del diritto o in casi particolarmente complessi entro 3 mesi;
2. *forma*: scritta, o anche in formato elettronico, eccetto il caso in cui l'interessato la richieda oralmente.
3. *contenuto*: sintetico, accessibile ed intellegibile.

L'unico obbligo in capo all'interessato è fornire i dati per la sua identificazione. La risposta in genere dovrebbe essere esente da costi, tranne l'eventuale rimborso del costo del supporto utilizzato. Nel caso di trattamenti basati sul consenso, comunque, prevale la possibilità di revoca del consenso rispetto al diritto di opposizione.

9. ALLEGATI

9.1. GDPR toolkit per i professionisti

L'allegato è costituito da un file excel, la cui versione 1.0 presenta le seguenti funzionalità:

- raccolta delle **informazioni del professionista** in qualità di titolare e/o responsabile del trattamento;
- raccolta delle **informazioni dei responsabili del trattamento designati** dal professionista;
- raccolta delle **informazioni sui soggetti autorizzati al trattamento** dal professionista;
- **inventario degli asset** a supporto delle attività di trattamento;
- suggerimento delle **misure di sicurezza adottabili** a riduzione del rischio;
- **redazione del registro delle attività di trattamento** in qualità di titolare e/o responsabile;
- descrizione delle **misure di sicurezza di sicurezza e valutazione dei rischi** connessi ad ogni trattamento dei dati personali;
- riepilogo delle informazioni sui trattamenti da presentare nelle **informative e nelle richieste di consenso** all'interessato.