COISPA Tecnologia e Ricerca S.c.r.l.

Sede legale: Bari (BA), via dei Trulli n. 18/20 - c.a.p. 70126

P.IVA/C.F.: 00934670720

N. telefono: 0805433596

E-mail: favia@coispa.eu

PEC: coispa@pec.coispa.it

REGOLAMENTO PRIVACY

STATO DELLE REVISIONI

Versione	Data	Descrizione
01	28/03/2022	Prima emissione
02	15/03/2023	Revisione

SOMMARIO

1. Premessa

L'attività lavorativa svolta da COISPA Tecnologia e Ricerca S.c.r.l. comporta la gestione di una serie di dati propri e di terzi, necessari per poter erogare le prestazioni contrattuali che vengono richiesti. Tali dati possono essere considerati "dati personali" quando sono riferite a persone fisiche.

Tali dati, quando sono riconducibili a persone fisiche, devono essere trattati nel pieno rispetto della normativa vigente in materia di privacy.

Altri dati, pur non essendo "dati personali" ai sensi di legge, sono in tutto e per tutto "informazioni riservate", ovvero informazioni tecniche, commerciali, contrattuali, di business o di altro genere per le quali il Titolare è chiamato a garantire la piena riservatezza per una più ampia tutela del proprio patrimonio.

In particolare, si ritiene necessario definire una chiara disciplina interna atta garantire che il trattamento dei dati svolto nell'ambito delle attività lavorative, avvenga in maniera conforme ai principi e alle disposizioni impartite dal Regolamento (UE) n. 2016/679 e dal d.lgs. 30 giugno 2003 n. 196 e s.m.i., in particolare ai criteri di liceità, correttezza e trasparenza.

Il corretto utilizzo degli strumenti, delle infrastrutture e delle informazioni trattate nei processi lavorativi costituisce una importante misura preventiva nei confronti dei rischi di violazione della riservatezza, integrità e disponibilità dei dati trattati.

In linea generale, ogni dato, nell'accezione più ampia sopra descritta, di cui i destinatari del presente documento vengono a conoscenza nell'ambito della propria attività lavorativa, è da considerarsi riservato e non deve essere comunicato o diffuso a nessuno (anche una volta interrotto il rapporto lavorativo con l'organizzazione stessa o qualora parte delle informazioni siano di pubblico dominio) salvo specifica autorizzazione esplicita.

Anche tra colleghi, oppure tra dipendenti e collaboratori esterni, è necessario adottare la più ampia riservatezza nella comunicazione dei dati conosciuti, limitandosi solo a quei casi che si rendono necessari per espletare al meglio l'attività lavorativa richiesta.

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, l'accesso alla rete internet dal computer di lavoro, espone il Titolare a possibili rischi di un coinvolgimento di rilevanza sia civile, sia penale, sia amministrativa, creando problemi alla sicurezza e all'immagine del Titolare stesso.

Una gestione dei dati cartacei, un uso di strumenti informatici e attrezzature elettroniche, nonché dei servizi internet e della posta elettronica difforme dalle regole contenute nel presente atto potrebbe esporre l'organizzazione ad aumentare la minaccia di accessi non autorizzati ai dati e/o al sistema informatico, furti o divulgazioni di informazioni riservate nonché furti o danneggiamenti del sistema informatico e/o malfunzionamenti in generale dell'intero sistema informatico.

Fermo restando che i comportamenti da adottare nell'ambito di un rapporto di lavoro o di un contratto - tra i quali rientrano il trattamento dei dati e l'utilizzo delle risorse informatiche e telematiche - devono sempre ispirarsi al principio di diligenza e correttezza, anche sulla scorta degli elementi su riportati, nel più ampio contesto della disciplina in materia di privacy, il Titolare ha elaborato e adottato il presente documento, diretto a evitare che condotte inconsapevoli possano innescare problemi o minacce alla sicurezza dei dati o delle attrezzature lavorative.

2. Scopo e ambito di applicazione

Lo scopo del presente documento è individuare le norme comportamentali e le procedure tecnico-organizzative cui è necessario attenersi in materia di trattamento di dati personali (e, più in generali, i dati lavorativi) nello svolgimento di tutte le attività lavorative, nel rispetto della normativa in materia di trattamento dei dati personali, garantendo in particolare l'aderenza ai principi e alle disposizioni di legge e preservando la riservatezza, l'integrità e la disponibilità dei dati e delle informazioni a tutela della dignità delle persone fisiche e delle libertà fondamentali.

Il presente regolamento è realizzato in conformità a quanto previsto dal Decreto Legislativo n. 196/2003 e s.m.i. (Codice in materia di protezione dei dati personali), dal Regolamento Europeo n. 2016/679 (*General Data Protection Regulation*), anche solo "GDPR", e dai Provvedimenti del Garante.

Sono destinatari del documento tutti i soggetti che, a qualsiasi titolo, trattano dati di competenza del Titolare del trattamento. A titolo esemplificativo:

- i lavoratori dipendenti, nonché coloro che, indipendentemente dal tipo di rapporto lavorativo intercorrente, abbiano accesso ai dati personali trattati nel corso del proprio impiego per conto del Titolare del trattamento (genericamente denominati autorizzati);
- i soggetti (persone fisiche o giuridiche) che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento, abbiano accesso ai suddetti dati e agiscano in qualità di Responsabile del trattamento ex art. 28 GDPR;
- tutti coloro che, anche mediante accesso alla rete informatica, utilizzano strumenti elettronici e soluzioni tecnologiche o usufruiscono di servizi la cui sicurezza è gestita dal Titolare del trattamento.

I destinatari devono obbligatoriamente attenersi al contenuto del presente regolamento. Fermi restando i profili di responsabilità diretta civile e penale previsti dalla normativa vigente, il mancato rispetto e la mancata conformità alle regole previste potrà comportare provvedimenti disciplinari a carico dei dipendenti inadempienti ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia, fermo restando il risarcimento di eventuali danni causati (cfr. par. 4.6).

A tal proposito, tutti i destinatari sono debitamente informati delle regole contenute nel presente documento mediante metodi e mezzi che ne assicurino la comprensione.

Il regolamento si applica alle attività che comportano il trattamento dei dati del Titolare (quali, ad es. attività connesse alla gestione del personale, agli organi societari e agli adempimenti relativi ai propri clienti, fornitori ed eventuali consulenti) ovvero alle attività eventuali che comportano il trattamento dei dati personali per le quali il Titolare operi, ai sensi dell'art. 28 del GDPR, in qualità di responsabile esterno del trattamento nel rispetto delle finalità determinate dai committenti e secondo le modalità previste dai contratti.

In merito all'utilizzo di software e banche dati, dove previsto, valgono le regole di tutela del diritto d'autore (Copyright).

Per quanto non espressamente disciplinato in questa sede, si rinvia ai principi e alle disposizioni del Regolamento Europeo, del Codice Privacy, ai Provvedimenti Generali, le Autorizzazioni Generali ed alle Linee Guida emanate dall'Autorità Garante per la Protezione dei dati personali e, più in generale, alla normativa vigente in tema di protezione dei dati.

3. Normativa di riferimento

Il presente documento è redatto in conformità alle disposizione di legge e alla normativa vigente. In particolare:

- Regolamento (UE) n. 2016/679;
- d.lgs. n. 196/2003;
- d.lgs. n. 101/2018.

3.1 Regolamento (UE) n. 2016/679

Il 14 aprile 2016, il Parlamento Europeo ha approvato il c.d. "pacchetto protezione dati" finalizzato alla definizione di un sistema armonizzato e un quadro operativo comune per tutti gli Stati membri dell'Unione Europea in materia di protezione dei dati personali.

Il "pacchetto" è composto da due diversi strumenti:

- Il Regolamento (UE) 2016/679 (c.d. GDPR – General Data Protection Regulation) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati;
- la Direttiva UE 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali.

Il GDPR è entrato in vigore il 24 maggio 2016 ed è diventato direttamente applicabile in ciascuno degli Stati Membri dell'Unione a decorrere dal 25 maggio 2018, con contestuale abrogazione della direttiva 95/46/CE.

Numerosi sono gli elementi innovativi contenuti nel GDPR:

- La definizione di "dato personale" è più dettagliata e comprende "qualsiasi informazione riguardante una persona fisica identificata o identificabile", ivi compresi gli indirizzi IP.
- Non esiste una definizione dei "dati sensibili", sostituita dalle "categorie particolari di dati personali" (dati genetici, dati biomedici, dati relativi alla salute etc.).
- È stato introdotto il principio di "***accountability***" (responsabilizzazione) dei titolari del trattamento: il Titolare avrà maggiore discrezionalità nel decidere come conformarsi alle disposizioni del Regolamento, ma avrà altresì l'onere di dimostrare le ragioni a supporto di tali decisioni.

- Non sono previste misure minime di sicurezza (come quelle disposte dalla precedente versione del codice privacy); tuttavia, sono previste "*misure tecniche e organizzative adeguate*", che comprendono, tra le altre: a) pseudonimizzazione e cifratura dei dati; b) garanzia su base permanente della riservatezza, integrità, disponibilità e resilienza dei servizi di trattamento; c) capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di *data breach*; d) procedura adeguata per testare, valutare e verificare l'efficacia delle misure tecniche e organizzative.

- Al fine di dimostrare la conformità al Regolamento, può essere utilizzata l'adesione al 'codice di condotta'. Oppure ad un meccanismo di 'certificazione': entrambi hanno natura volontaria.

- Sono stati accresciuti gli obblighi di trasparenza e informativi: le informazioni agli interessati devono essere date con un linguaggio semplice e chiaro, soprattutto nel caso di minore di anni 16.

- Sono stati introdotti i concetti di ***privacy by design*** e ***privacy by default***: sarà necessario adottare misure tecniche e organizzative adeguate sin dal momento della progettazione e per impostazione predefinita.

- Sia il titolare che il responsabile del trattamento devono tenere un **registro delle attività del trattamento**, in forma scritta, anche in formato elettronico, in cui è possibile inserire le misure di sicurezza tecniche e organizzative adottate.

- ***Data breach notification***: In caso di violazione dei dati personali, qualora ricorrano determinati presupposti, il Titolare è tenuto a notificare la violazione al Garante senza ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza.

- Qualora un tipo di trattamento dei dati presenti un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento deve effettuare, prima di procedere al trattamento una **valutazione d'impatto (DPIA)**.

- Il GDPR riconosce espressamente il diritto alla cancellazione permettendo all'interessato di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano (**diritto all'oblio**).

- È stata introdotta la figura del **DPO (*Data Protection Officer*)** che svolgerà un ruolo di consulenza, controllo e audit, nonché di cooperazione con il Garante nei confronti del soggetto che l'avrà nominato (Titolare o Responsabile del trattamento).

3.1.1 Ambito di applicazione

L'ambito di applicazione del GDPR è così disciplinato:

Ambito di applicazione materiale

Ai sensi dell'art. 2, il 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*".

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;

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.

Applicazione territoriale

Ai sensi dell'art. 3, il 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*".

Ancora, dispone la norma, il 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*."

3.1.2 Definizioni

Ai sensi dell'art.4 del Regolamento s'intende per:

«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;

«trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

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

«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;

«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;

«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;

«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;

«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;

«destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

«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;

«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;

«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;

«dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

«dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne

consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

«dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

«stabilimento principale»:

a) 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;

b) 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 GDPR;

«rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27 del GDPR, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del GDPR;

«impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

«gruppo imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

«norme vincolanti d'impresa»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi

terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

«autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

«autorità di controllo interessata»: un'autorità di controllo interessata dal trattamento di dati personali in quanto:

a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;

b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure

c) un reclamo è stato proposto a tale autorità di controllo;

«trattamento transfrontaliero»:

a) 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

b) 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;

«obiezione pertinente e motivata»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del GDPR, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al GDPR, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

«servizio della società dell'informazione»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio;

«organizzazione internazionale»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

3.1.3 Principi

Ai sensi dell'art. 5 del GDPR, 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) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («**minimizzazione dei dati**»);
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**»).

<u>Liceità del trattamento:</u>

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.

Condizioni per il consenso:

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.

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.

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

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.

Trattamento di categorie particolari di dati personali:

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.

Possono essere trattati nei seguenti casi:

- 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 trattamento;
- 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;
- 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 è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;
- il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
- il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
- 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;
- 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;
- il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei

dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;

- il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità al GDPR, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Queste categorie particolari di dati personali possono essere trattate se i 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.

Il trattamento dei dati personali relativi alle condanne penali e ai reati deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.

3.1.4 Soggetti coinvolti nei trattamenti

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.

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 GDPR. Dette misure sono riesaminate e aggiornate qualora necessario.

Se ciò è proporzionato rispetto alle attività di trattamento, le misure tecniche e organizzative adottate includeranno l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.

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'adesione ai codici di condotta o a un meccanismo di certificazione può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

Contitolare del trattamento:

Il GDPR ha introdotto la figura del contitolare del trattamento, vale a dire il soggetto che determina congiuntamente al titolare le finalità e i mezzi del trattamento. Entrambi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni previste dalla normativa, 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. Questi ultimi possono esercitare i propri diritti ai sensi del GDPR nei confronti di e contro ciascun titolare del trattamento.

La protezione dei diritti e delle libertà degli interessati così come la responsabilità generale dei titolari del trattamento e dei responsabili del trattamento, anche in relazione al monitoraggio e alle misure delle autorità di controllo, esigono una chiara ripartizione delle responsabilità ai sensi del GDPR , compresi i casi in cui un titolare del trattamento stabilisca

le finalità e i mezzi del trattamento congiuntamente con altri titolari del trattamento o quando l'operazione di trattamento viene eseguita per conto del titolare del trattamento.

Responsabile della protezione dei dati (RPD):

L'art. 37, par. 1, lett. a), del GDPR prevede che i titolari e i responsabili del trattamento designino un RPD (in inglese "*Data Protection Officer*", di seguito anche solo DPO) «*quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali*».

A titolo esemplificativo e non esaustivo, in ambito pubblico, devono ritenersi tenuti alla designazione di un DPO le amministrazioni dello Stato, anche con ordinamento autonomo, gli enti pubblici non economici nazionali, regionali e locali, le Regioni e gli enti locali, le Università, le Camere di commercio, industria, artigianato e agricoltura, le aziende del Servizio sanitario nazionale, le autorità indipendenti, etc..

Occorre, comunque, considerare che, nel caso in cui soggetti privati esercitino funzioni pubbliche (in qualità, ad esempio, di concessionari di servizi pubblici), può risultare comunque fortemente raccomandato, ancorché non obbligatorio, procedere alla designazione di un DPO. In ogni caso, qualora si proceda alla designazione di un DPO su base volontaria, si applicano gli identici requisiti - in termini di criteri per la designazione, posizione e compiti - che valgono per i DPO designati in via obbligatoria.

Ancora, l'art. 2-sexiesdecies ("*Responsabile della protezione dei dati per i trattamenti effettuati dalle autorità giudiziarie nell'esercizio delle loro funzioni*"), aggiunto in una fase successiva dell'*iter* travagliato che ha caratterizzato il decreto di adeguamento n. 101/2018, ha introdotto l'obbligo anche per le autorità giudiziarie di designare il DPO, previsione che ricalca quanto già stabilito dal d.lgs. 18 maggio 2018, n. 51, approvato nel maggio 2018, in attuazione alla direttiva (UE) 2016/680.

Quanto all'ambito privato, sono tenuti alla designazione del DPO il titolare e il responsabile del trattamento che rientrino nei casi previsti dall'art. 37, par. 1, lett. b) e c), del Regolamento (UE) 2016/679. Si tratta di soggetti le cui principali attività (*in primis*, le attività c.d. di "*core business*") consistono in trattamenti che richiedono il **monitoraggio regolare e sistematico degli interessati su larga scala** o in trattamenti **su larga scala** di categorie particolari di dati personali o di dati relative a condanne penali e a reati (per quanto attiene alle nozioni di "monitoraggio regolare e sistematico" e di "larga scala", cfr. le "Linee guida sui responsabili della protezione dei dati" del 5 aprile 2017, WP 243). Il diritto dell'Unione o

degli Stati membri può prevedere ulteriori casi di designazione obbligatoria del responsabile della protezione dei dati (art. 37, par. 4).

Ricorrendo i suddetti presupposti, sono tenuti alla nomina, a titolo esemplificativo e non esaustivo: istituti di credito; imprese assicurative; sistemi di informazione creditizia; società finanziarie; società di informazioni commerciali; società di revisione contabile; società di recupero crediti; istituti di vigilanza; partiti e movimenti politici; sindacati; CAF e patronati; società operanti nel settore delle "utilities" (telecomunicazioni, distribuzione di energia elettrica o gas); imprese di somministrazione di lavoro e ricerca del personale; società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione; società di call center; società che forniscono servizi informatici; società che erogano servizi televisivi a pagamento (sul tema, cfr. le "*Nuove Faq sul Responsabile della Protezione dei Dati (RPD) in ambito privato*" del Garante).

Il Regolamento prevede che un gruppo imprenditoriale (art. 4, n. 19) possa designare un unico DPO, purché questi sia facilmente raggiungibile da ciascuno stabilimento. Per garantire tale accessibilità si raccomanda che il DPO sia localizzato nel territorio dell'Unione europea, indipendentemente dal fatto che il titolare del trattamento o il responsabile del trattamento siano stabiliti nell'UE. Tuttavia, non si può escludere che, in alcuni casi ove il titolare del trattamento o il responsabile del trattamento non sono stabiliti nell'UE, un DPO sia in grado di svolgere i propri compiti con maggiore efficacia operando al di fuori del territorio dell'UE.

Inoltre, dovrà essere in grado di comunicare in modo efficace con gli interessati e di collaborare con le autorità di controllo.

Il ruolo di DPO può essere ricoperto da un dipendente del titolare o del responsabile (non in conflitto di interessi) che conosca la realtà operativa in cui avvengono i trattamenti; l'incarico può essere anche affidato a soggetti esterni, a condizione che garantiscano l'effettivo assolvimento dei compiti che il Regolamento assegna a tale figura.

Il DPO scelto all'interno andrà nominato mediante specifico atto di designazione, mentre quello scelto all'esterno, che dovrà avere le medesime prerogative e tutele di quello interno, dovrà operare in base a un contratto di servizi. Tali atti, da redigere in forma scritta, dovranno indicare espressamente i compiti attribuiti, le risorse assegnate per il loro svolgimento, nonché ogni altra utile informazione in rapporto al contesto di riferimento.

Nell'esecuzione dei propri compiti, il DPO (interno o esterno) dovrà ricevere supporto adeguato in termini di risorse finanziarie, infrastrutturali e, ove opportuno, di personale. Il

titolare o il responsabile del trattamento che abbia designato un DPO resta comunque pienamente responsabile dell'osservanza della normativa in materia di protezione dei dati e deve essere in grado di dimostrarla.

I dati di contatto del DPO designato dovranno essere infine pubblicati dal titolare o responsabile del trattamento. Non è necessario - anche se potrebbe rappresentare una buona prassi - pubblicare anche il nominativo del DPO: spetta al titolare o al responsabile e allo stesso responsabile della protezione dei dati, valutare se, in base alle specifiche circostanze, possa trattarsi di un'informazione utile o necessaria. Il nominativo del DPO e i relativi dati di contatto vanno invece comunicati all'Autorità di controllo.

È opportuno, in primo luogo, valutare se il complesso dei compiti assegnati al DPO - aventi rilevanza interna (consulenza, pareri, sorveglianza sul rispetto delle disposizioni) ed esterna (cooperazione con l'autorità di controllo e contatto con gli interessati in relazione all'esercizio dei propri diritti) - siano (o meno) compatibili con le mansioni ordinariamente affidate ai dipendenti.

In merito, l'art. 38, par. 3, del GDPR fissa alcune garanzie essenziali per consentire ai DPO di operare con un grado sufficiente di autonomia all'interno dell'organizzazione. In particolare, occorre assicurare che il DPO "*non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti*". Il considerando 97 aggiunge che i DPO "*dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente*". Ciò significa, come chiarito nelle Linee guida, che «*il DPO, nell'esecuzione dei compiti attribuitigli ai sensi dell'articolo 39, non deve ricevere istruzioni sull'approccio da seguire nel caso specifico – quali siano i risultati attesi, come condurre gli accertamenti su un reclamo, se consultare o meno l'autorità di controllo. Né deve ricevere istruzioni sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati*».

Inoltre, sempre ai sensi dell'art. 38, par. 3, del GDPR, il DPO «*riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento*». Tale rapporto diretto garantisce, in particolare, che il vertice amministrativo venga a conoscenza delle indicazioni e delle raccomandazioni fornite dal DPO nell'esercizio delle funzioni di informazione e consulenza a favore del titolare o del responsabile.

Alla luce delle considerazioni di cui sopra, nel caso in cui si opti per un DPO interno, sarebbe quindi in linea di massima preferibile che, ove la struttura organizzativa lo consenta e tenendo conto della complessità dei trattamenti, la designazione sia conferita a un dirigente ovvero a un funzionario di alta professionalità, che possa svolgere le proprie funzioni in

autonomia e indipendenza, nonché in collaborazione diretta con il vertice dell'organizzazione.

Appare preferibile evitare di assegnare il ruolo di DPO a soggetti con incarichi di alta direzione (amministratore delegato; membro del consiglio di amministrazione; direttore generale; ecc.), ovvero nell'ambito di strutture aventi potere decisionale in ordine alle finalità e alle modalità del trattamento (direzione risorse umane, direzione marketing, direzione finanziaria, responsabile IT ecc.). Da valutare, in assenza di conflitti di interesse e in base al contesto di riferimento, l'eventuale assegnazione di tale incarico ai responsabili delle funzioni di staff (ad esempio, il responsabile della funzione legale).

Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:

- 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;
- 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;
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
- cooperare con l'autorità di controllo; e
- fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

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.

Responsabile del trattamento:

Ai sensi dell'art. 28 del GDPR, 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 GDPR e garantisca la tutela dei diritti dell'interessato.

Il responsabile del trattamento può avvalersi di sub-responsabili 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.

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 di sicurezza richieste dal GDPR;
d) rispetti le condizioni su esposte 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;
f) assista il titolare del trattamento nel garantire il rispetto degli obblighi previsti dal GDPR, 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), il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il GDPR o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

L'adesione da parte del responsabile del trattamento a un codice di condotta approvato o a un meccanismo di certificazione approvato può essere utilizzata come elemento per dimostrare le garanzie sufficienti di sicurezza.

Fatto salvo un contratto individuale tra il titolare del trattamento e il responsabile del trattamento, il contratto o altro atto giuridico può basarsi, in tutto o in parte, su clausole contrattuali tipo, anche laddove siano parte di una certificazione concessa al titolare del trattamento o al responsabile del trattamento.

In tale ottica, tanto la Commissione secondo la procedura d'esame quanto un'autorità di controllo possono stabilire clausole contrattuali tipo per le materie di cui sopra.

Il contratto o altro atto giuridico è stipulato in forma scritta, anche in formato elettronico.

Se un responsabile del trattamento viola le disposizioni dettate dal Titolare determinando le finalità e i mezzi del trattamento, è considerato un autonomo Titolare del trattamento in questione.

Sub-Responsabile:

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 (sub.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, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR. 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 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.

Autorizzato:

Pur non prevedendo espressamente la figura dell'«*incaricato*» del trattamento (figura disciplinata dal d.lgs. 196/2003 nella precedente versione), il regolamento non ne esclude la presenza. Nella norma sovranazionale, infatti, è presente il riferimento a «*persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile*» (cfr. artt. 4, n. 10), e 29).

Il soggetto autorizzato (ex "*incaricato*") è una figura di primissima rilevanza nell'organigramma privacy di qualsiasi struttura poiché è colui il quale, sotto la diretta autorità del titolare e del responsabile (se nominato), dietro apposita autorizzazione, effettua materialmente le operazioni di trattamento sui dati personali.

Sul tema, il nuovo testo del Codice Privacy (d.lgs. 196/2003), così come modificato dal d.lgs. n. 101/2018, all'art. 2-quaterdecies rubricato "*Attribuzione di funzioni e compiti a soggetti designati*", dispone che:

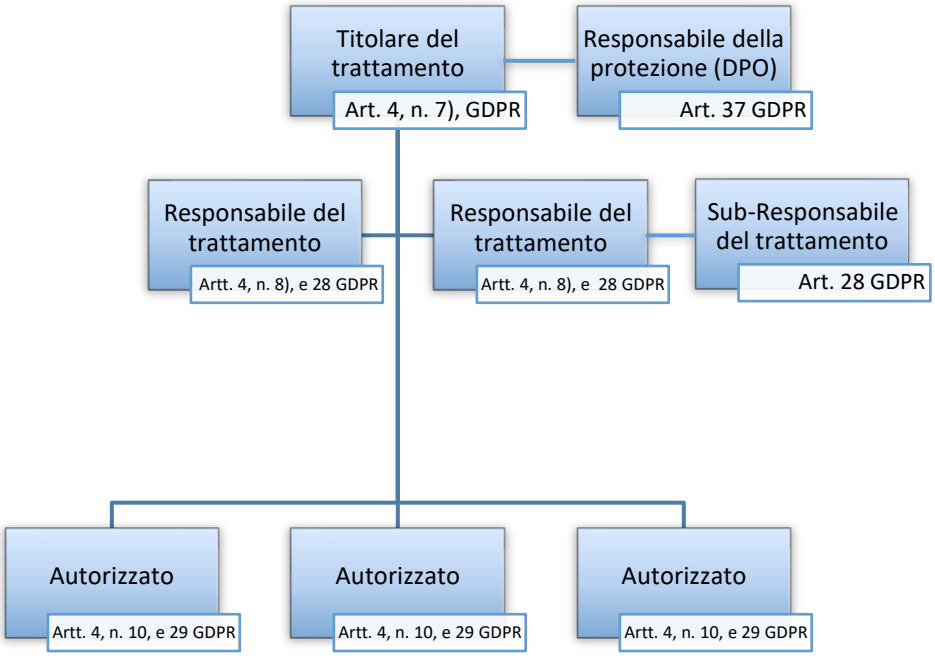
"*Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto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

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".

Tale norma, sembra esplicitare ulteriormente la presenza della figura dello "*autorizzato*", corrispondente al precedente "*incaricato*".

Per quanto riguarda le modalità e le direttive cui i soggetti summenzionati devono attenersi nel trattamento dei dati, si rimanda ai paragrafi successivi.

Organigramma tipo:



3.1.5 Registro delle attività di trattamento

Per dimostrare che si conforma al GDPR, il titolare del trattamento o il responsabile del trattamento che abbia più di 250 dipendenti deve tenere un registro delle attività di trattamento effettuate sotto la sua responsabilità.

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:

- 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;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- 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 la documentazione delle garanzie adeguate;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

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:

- 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;
- le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
- 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 la documentazione delle garanzie adeguate;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

I registri del trattamento sono tenuti in forma scritta, anche in formato elettronico.

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.

Tali obblighi 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 che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, di dati genetici, biometrici, dati relativi alla salute, alla vita o all'orientamento sessuale o di dati relativi a condanne penali e a reati.

La tenuta dei registri di trattamenti non costituisce un adempimento formale, bensì parte integrante di un sistema di corretta gestione dei dati personali. Per tale motivo, è consigliabile che tutti i titolari e i responsabili del trattamento, a prescindere dalle dimensioni dell'organizzazione, si dotino del registro dei trattamenti e, in ogni caso, compiano un'accurata ricognizione dei trattamenti svolti e delle caratteristiche.

nometitolare a prescindere dal numero dei dipendenti presenti, ha stabilito di elaborare e adottare un registro delle attività di trattamento, anche nell'ottica di facilitare la cooperazione con l'Autorità di controllo e mettere, su richiesta, detto registro a sua disposizione affinché possano servire per monitorare i trattamenti effettuati.

3.1.6 Analisi dei rischi e valutazione d'impatto (DPIA)

Il titolare del trattamento è tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il GDPR, compresa l'efficacia delle misure.

Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.

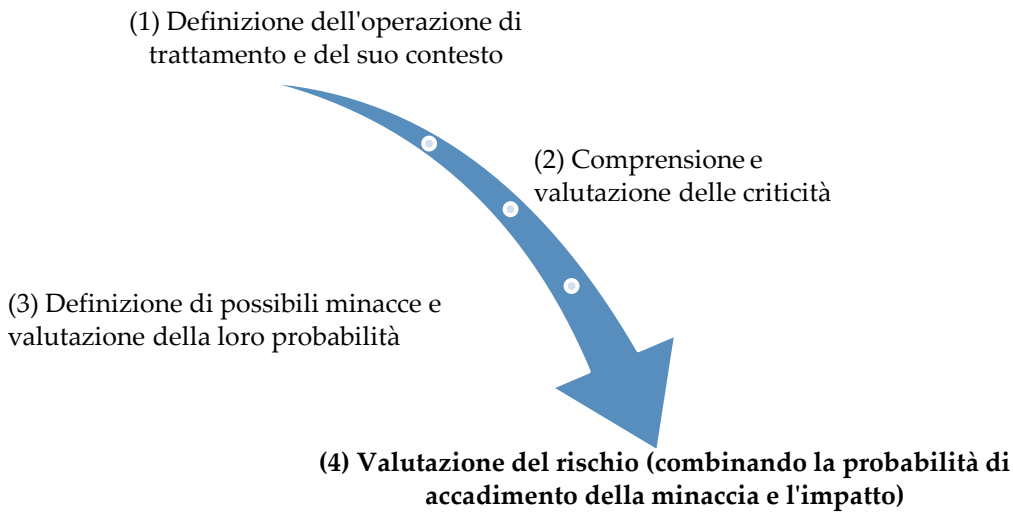
I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali

che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di 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; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato.

Le difficoltà decisionali, di gestione del rischio consistono, quindi, nel trovare un equilibrio tra sicurezza e vincoli organizzativi o tra sicurezza e complessità. In sostanza, il sistema di sicurezza deve trovare un equilibrio tra costo della protezione e valore del bene protetto, bilanciato da un eguale equilibrio tra complessità del sistema e vincoli che sono posti per renderlo sicuro.

Nello specifico, il metodo per l’analisi di base del Titolare, relativo ai trattamenti per i quali non è richiesta una valutazione d’impatto (art. 35 del GDPR), è realizzato tramite un processo per fasi in riferimento allo schema di seguito riportato, presente anche sul registro delle attività di trattamento, il cui strumento di valutazione è formato da un sistema tabellare, che determina il grado di rischio cui il sistema e le strutture sono sottoposti, nonché la definizione di misure di sicurezza adeguate e giustificate.



Fase 1: Definizione dell'operazione di trattamento e del suo contesto

Questo passaggio è il punto di partenza della valutazione del rischio. Si effettua circoscrivendo la tipologia di operazione che il Titolare effettua sul dato (lettura, modifica, cancellazione etc.) e la finalità della stessa, combinando il tutto con i dati che sono effettivamente oggetto di trattamento.

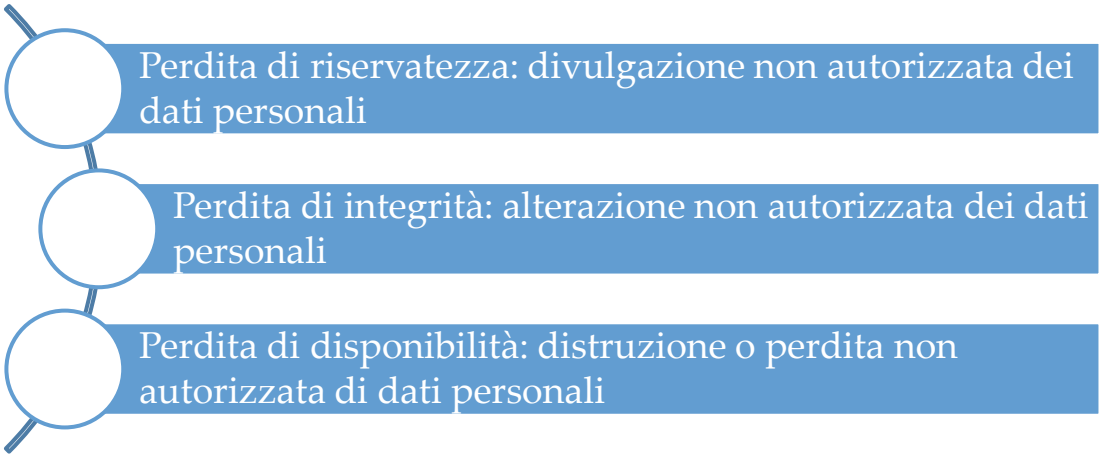
Una volta definito questo, si individuano il luogo e gli strumenti dedicati al trattamento ed infine le categorie di soggetti interessati ed i destinatari dei dati.

Fase 2: Comprensione e valutazione delle criticità

Il Titolare del trattamento in questa fase deve valutare il rischio gravante sui diritti e sulle libertà fondamentali delle persone fisiche derivante dalla possibile perdita di sicurezza dei dati personali.

Il Titolare del trattamento è tenuto a considerare una serie di fattori, tutti precedentemente individuati (*vedi Fase 1*) quali ad es. la tipologia di dati personali, le operazioni di trattamento, la strumentazione ed il luogo in cui le operazioni vengono effettuate, così come anche le speciali categorie di interessati.

In questa fase è bene riflettere sull'impatto che una perdita di sicurezza dei dati potrebbe avere sull'individuo ed esprimere una valutazione di conseguenza. Le possibili criticità da analizzare sono tre:



Indicativamente, all'esito della valutazione possono raggiungersi quattro possibili livelli di rischio:

Basso	• Gli individui possono andare incontro a disagi minori, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.).
Medio	• Gli individui possono andare incontro a significativi disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.).
Alto	• Gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, ecc.).
Molto alto	• Gli individui possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).

Fase 3: Definizione di possibili minacce e valutazione della loro probabilità

In questa fase lo scopo del Titolare del trattamento è comprendere le minacce correlate al contesto complessivo del trattamento dei dati personali (esterno o interno) e valutare la loro probabilità (probabilità di accadimento della minaccia).

Per una corretta valutazione è necessario considerare:

1. Risorse di rete e tecniche (strumentazione hardware e software);

2. Processi / procedure relativi all'operazione di trattamento dei dati;

3. Diverse parti e persone coinvolte nell'operazione di trattamento;

4. Settore di operatività e scala del trattamento.

All'esito di quest'ultima analisi, il livello di probabilità di occorrenza della minaccia può essere definito come segue:

Basso	• è improbabile che la minaccia si materializzi.
Medio	• c'è una ragionevole possibilità che la minaccia si materializzi.
Alto	• la minaccia potrebbe materializzarsi.

Fase 4: Valutazione del rischio

Dopo aver valutato l'impatto dell'operazione di trattamento dei dati personali e la probabilità di accadimento della minaccia rilavante, la valutazione finale del rischio è possibile.

	BASSO	MEDIO	ALTO/MOLTO ALTO
BASSO			
MEDIO			
ALTO			

= Rischio basso

= Rischio medio

= Rischio alto

Tale schema risulta semplificato rispetto a quello utilizzato per la valutazione d'impatto di seguito descritta.

Valutazione d'impatto

Quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate (a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono magari trattati dati sensibili, o anche per una combinazione di questi e altri fattori), il regolamento 2016/679 obbliga i titolari a svolgere una valutazione di impatto prima di darvi inizio, consultando l´autorità di controllo in caso le misure tecniche e organizzative da loro stessi individuate per mitigare l´impatto del trattamento non siano ritenute sufficienti - cioè, quando il rischio residuale per i diritti e le libertà degli interessati resti elevato.

Si tratta di uno degli elementi di maggiore rilevanza nel nuovo quadro normativo, perché esprime chiaramente la responsabilizzazione (*accountability*) dei titolari nei confronti dei trattamenti da questi effettuati. I titolari sono infatti tenuti non soltanto a garantire l´osservanza delle disposizioni del regolamento, ma anche a dimostrare adeguatamente in che modo garantiscono tale osservanza; la valutazione di impatto ne è un esempio.

La DPIA rappresenta quindi un processo con il quale verificare che siano garantiti i principi della cosiddetta triade: Confidenzialità, Integrità e Disponibilità del dato. Pertanto con la DPIA si verificherà l'impatto sulla privacy di un progetto, una scelta, una policy, un software, un servizio, un dispositivo, un prodotto o comunque tutte quelle iniziative che coinvolgono il trattamento di dati personali al fine di mitigare, minimizzare i potenziali rischi. Per condurre un DPIA è indispensabile un approccio multidisciplinare che valuti tutte le fasi ed i soggetti coinvolti nel trattamento. Non solo valutazioni tecnologiche, quindi, ma anche e soprattutto organizzative.

Ai sensi dell'art. 35 del GDPR, la valutazione d'impatto sulla protezione dei dati è richiesta in particolare nei casi seguenti:

- una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- il trattamento, su larga scala, di categorie particolari di dati personali rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, di dati genetici, biometrici, dati relativi alla salute, alla vita o all'orientamento sessuale o di dati relativi a condanne penali e a reati;
- la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Laddove la valutazione d'impatto sulla protezione dei dati indichi che i trattamenti presentano un rischio elevato che il titolare del trattamento non può attenuare mediante misure opportune in termini di tecnologia disponibile e costi di attuazione, prima del trattamento si dovrebbe consultare l'autorità di controllo.

Le linee-guida del WP29 offrono alcuni chiarimenti sul punto; in particolare, precisano quando una valutazione di impatto sia obbligatoria (oltre ai casi espressamente indicati dal regolamento all´art. 35), chi debba condurla (il titolare, coadiuvato dal responsabile della protezione dei dati, se designato), in cosa essa consista (fornendo alcuni esempi basati su schemi già collaudati in alcuni settori), e la necessità di interpretarla come un processo soggetto a revisione continua piuttosto che come un adempimento una tantum.

Le linee-guida chiariscono, peraltro, anche quando una valutazione di impatto non sia richiesta: ciò vale, in particolare, per i trattamenti in corso che siano già stati autorizzati dalle autorità competenti e non presentino modifiche significative prima del 25 maggio 2018, data di piena applicazione del regolamento.

La DPIA contiene almeno:

- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati;
- 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 GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Grazie alla DPIA si è in grado di definire il rischio residuo che il titolare potrebbe decidere di accettare o potrebbe decidere di trasferire il rischio attraverso l'attivazione di specifiche coperture assicurative.

3.1.7 Misure di sicurezza

A seguito dell'analisi dei rischi effettuata, il Titolare stabilisce le misure di sicurezza adeguate.

Le misure di sicurezza scelte e adottate dal titolare e/o dal responsabile del trattamento devono essere in grado di garantire:

- **riservatezza**: garanzia che l'accesso ai dati sia consentito solo ai soggetti legittimati;
- **integrità**: garanzia che la modifica dei dati venga effettuata solo da parte dei soggetti autorizzati;

- **disponibilità**: garanzia che il sistema e i dati siano accessibili con continuità.

A differenza del d.lgs. 196/03 e, in particolare dell'abrogato Allegato B, il GDPR non presenta delle misure minime di protezione da adottare per garantire un adeguato trattamento, ma stabilisce che i dati siano 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»).

L'art. 32 del GDPR, tuttavia, prescrive che il titolare del trattamento e il responsabile del trattamento debbano mettere in atto misure tecniche e organizzative **adeguate** per garantire un livello di sicurezza adeguato al rischio, che comprendano, tra le altre, se del caso:

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

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.

Quanto espresso nell'art. 32 richiama espressamente ad una delle novità principali del GDPR: la Privacy by Design, intesa come Protezione dei dati fin dalla progettazione: 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 GDPR e tutelare i diritti degli interessati.

Un processo di Privacy by Design deve valutare l'intero processo del trattamento:

- dall'acquisizione dei dati all'eventuale distruzione (se prevista);

- degli strumenti utilizzati per la memorizzazione e gestione (cartacea o elettronica);
- della valutazione dei rischi e delle probabilità che incombono sul trattamento;
- delle misure di sicurezza fisiche, tecniche ed organizzative adottate;
- della valutazione dei rischi residui.

Alla Privacy by Design il GDPR associa la Privacy by Default: 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.

3.1.8 *Data breach*

L'art. 33 del Regolamento Europeo 679/2016 (GDPR) impone al titolare del trattamento di notificare all'autorità di controllo la violazione di dati personali (data breach) entro 72 ore dal momento in cui ne viene a conoscenza.

L'obbligo di notifica scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche, qualora, poi, il rischio fosse elevato, allora, oltre alla notifica, il titolare è tenuto a darne comunicazione all'interessato.

Il termine per adempiere alla notifica è brevissimo, 72 ore dal momento in cui il titolare ne viene a conoscenza, mentre, l'eventuale comunicazione agli interessati, deve essere fatta senza indugio.

L'eventuale ritardo nella notificazione deve essere giustificato, il mancato rispetto dell'obbligo di notifica, invece, pone l'autorità di controllo nella condizione di applicare le misure correttive a sua disposizione ovvero: l'esercizio dei poteri previsti dall'art.58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati), la imposizione di sanzioni amministrative secondo il GDPR.

Per "Violazione di dati" si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

La violazione di dati è un particolare tipo di incidente di sicurezza, per effetto del quale, il titolare non è in grado di garantire il rispetto dei principi prescritti dal GDPR per il trattamento dei dati personali.

Preliminarmente, dunque, il titolare deve poter identificare l'incidente di sicurezza in genere, quindi, comprendere che l'incidente ha impatto sulle informazioni e, infine, che tra le informazioni coinvolte dall'incidente vi sono dati personali.

L'art. 33 del GDPR prescrive al titolare di documentare qualsiasi violazione dei dati personali, al fine di consentire all'autorità di controllo di verificare il rispetto della norma e prevede espressamente il dovere per il responsabile, quando viene a conoscenza di una violazione, di informare, senza ingiustificato ritardo, il titolare.

È importante che sia dimostrabile il momento della scoperta dell'incidente, poiché da quel momento decorrono le 72 ore per la notifica.

Si possono distinguere tre tipi di violazioni:

- violazione di riservatezza, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale;
- violazione di integrità, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale;
- violazione di disponibilità, ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.

Una violazione potrebbe comprendere una o più tipologie.

Per comprendere quando notificare la violazione è opportuno effettuare una valutazione dell'entità dei rischi:

- Rischio assente: la notifica al Garante non è obbligatoria.
- Rischio presente: è necessaria la notifica al Garante.
- Rischio elevato: In presenza di rischi "elevati", è necessaria la comunicazione agli interessati. Nel momento in cui il titolare del trattamento adotta sistemi di crittografia dei dati, e la violazione non comporta l'acquisizione della chiave di decrittografia, la comunicazione ai soggetti interessati non sarà un obbligo.

I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
- riguardare categorie particolari di dati personali;

- comprendere dati che possono accrescere ulteriormente i potenziali rischi (es. dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
- comportare rischi imminenti e con un'elevata probabilità di accadimento (es. rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (es. pazienti, minori, soggetti indagati).

Per ogni ulteriore informazione sul tema, si rinvia alla *policy* dedicata.

3.1.9 Sanzioni

Le conseguenze derivanti da un inadempimento o da un *data breach,* oltre che creare nocumento all'interessato espone l'organizzazione a un danno di immagine e a rilevanti sanzioni amministrative e penali.

Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie siano in ogni singolo caso effettive, proporzionate e dissuasive.

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

o 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;

- il carattere doloso o colposo della violazione;
- le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;
- 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;
- eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;
- il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;
- le categorie di dati personali interessate dalla violazione;
- 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;

- qualora siano stati precedentemente disposti provvedimenti nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;
- l'adesione ai codici di condotta;
- 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.

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 GDPR, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave.

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:

- gli obblighi del titolare del trattamento e del responsabile del trattamento;
- gli obblighi dell'organismo di certificazione;
- gli obblighi dell'organismo di controllo.

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:

- i principi di base del trattamento, comprese le condizioni relative al consenso;
- i diritti degli interessati;
- i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale;
- qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate;
- 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.

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.

L'esercizio da parte dell'autorità di controllo dei poteri attribuitile dal GDPR è soggetto a garanzie procedurali adeguate in conformità del diritto dell'Unione e degli Stati membri, inclusi il ricorso giurisdizionale effettivo e il giusto processo.

Se l'ordinamento giuridico dello Stato membro non prevede sanzioni amministrative pecuniarie, le sanzioni presentate nel GDPR possono essere applicate 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.

Le sanzioni penali sono disciplinate dalla normativa nazionale.

3.2 Normativa italiana

In Gazzetta Ufficiale del 04 settembre 2018 è stato pubblicato il decreto di adeguamento della normativa italiana al Regolamento UE 2016/679 (GDPR).

Il decreto, composto da 27 articoli, è entrato in vigore il 19 settembre 2018.

Il complesso e lungo iter che ha portato all'approvazione del decreto ha attraversato due distinte legislature, passando dalla scelta iniziale di abrogare l'intero Codice Privacy a una successiva decisione di novellare il contenuto del d.lgs. 196/2003.

La scelta legislativa intrapresa dal legislatore nazionale, tuttavia, pone non pochi problemi interpretativi.

Di seguito è riportata una breve carrellata delle novità principali introdotte dal decreto.

Poteri e compiti del Garante

Il decreto, di fatto, si limita ad adeguare il testo del d.lgs. 196/2003 alle disposizioni previste dal Regolamento UE 2016/679, senza tuttavia entrare nel merito di alcuni dei punti più complessi del Regolamento.

Pertanto, il Garante italiano è chiamato a compiere un lavoro enorme di coordinamento del sistema normativo composto dal GDPR, dal decreto di adeguamento e dal novellato d.lgs. 196/2003.

Per quanto riguarda i provvedimenti del Garante già emessi, essi continueranno ad essere efficaci in quanto compatibili.

E' prevista, inoltre, una procedura di riesame e revisione delle autorizzazioni generali e dei codici deontologici allegati al Codice della privacy.

Curriculum vitae

L'art. 9 introduce nel d.lgs. 196/2003 l'art 111-bis (Informazioni in caso di ricezione di curriculum) stabilendo che "*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, paragrafo 1, lettera b), del Regolamento, il consenso al trattamento dei dati personali presenti nei curricula non è dovuto.*"

Consenso del minore

Perché sia lecito il trattamento dei dati nell'ambito dell'offerta diretta di servizi della società dell'informazione ai minori, ai sensi dell'art. 8 del GDPR, il minore deve avere almeno 16 anni. Diversamente, il consenso deve essere prestato o autorizzato dal titolare della responsabilità genitoriale. Lo stesso Regolamento concede la possibilità agli Stati membri di stabilire un'età inferiore purché non sotto i 13 anni. Orbene, l'art. 2-quinquies (Consenso del minore in relazione ai servizi della società dell'informazione) fissa come età minima di validità del consenso 14 anni. A tal proposito, le informazioni relative al trattamento devono essere redatte "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".

Per i minori di età inferiore è necessario che il consenso sia prestato da chi esercita la responsabilità genitoriale.

Categorie particolari di dati personali in ambito sanitario

Particolarmente interessante è la revisione della disciplina relativa al trattamento di dati personali in ambito sanitario. L'art. 6 del decreto 101/2018, infatti, ridisegna la parte II del titolo V del d.lgs. n. 196/2003 in conformità alle previsioni del GDPR (art. 9) eliminando la necessità del consenso per il trattamento di categorie particolari di dati personali in ambito sanitario.

In ogni caso, il trattamento dei dati genetici, biometrici e relativi alla salute dovrà avvenire in conformità alle misure di garanzia disposte dal garante con cadenza biennale (art. 2-septies del Codice Privacy). Tali misure individuano le misure di sicurezza, ivi comprese quelle tecniche di cifratura e di pseudonimizzazione, le misure di minimizzazione, le specifiche modalità per l'accesso selettivo ai dati e per rendere le informazioni agli interessati, nonché le eventuali altre misure necessarie a garantire i diritti degli interessati.

Tutela di fronte al Garante

Con la novella del decreto 101/2018 viene meno il Ricorso quale forma di tutela dinanzi al Garante.

In alternativa alla tutela giurisdizionale persiste il Reclamo (art. 141 e ss. del codice Privacy), novellato dall'art. 13 del decreto di adeguamento, il cui procedimento di esame sarà disciplinato dal Garante con proprio regolamento.

Particolarmente rilevante è la disciplina delle segnalazioni (richiamate nell'art. 54, par. 2, del GDPR), contenuta direttamente dal novellato art. 144. Il succitato articolo, infatti, stabilisce che "Chiunque" possa rivolgere una segnalazione al Garante e non i soli interessati come previsto dalla lettura combinata dei previgenti testi degli art. 142 e 144 del Codice.

Regime sanzionatorio

L'art. 18 del decreto di adeguamento, in deroga all'articolo 16 della legge 24 novembre 1981, n. 689, introduce la possibilità di definire i procedimenti pendenti relativi a violazioni amministrative del vecchio codice Privacy, con il pagamento in misura ridotta di una somma pari a due quinti del minimo edittale. Tale pagamento deve avvenire entro 90 giorni dall'entrata in vigore del d.lgs. n. 101/2018 (19 settembre 2018).

In virtù della "depenalizzazione" operata dal GDPR rispetto alle disposizioni del previgente Codice Privacy, con conseguente inasprimento delle sanzioni amministrative, il legislatore ha abrogato le sanzioni penali sovrapponibili a quelle amministrative (artt. 161, 162, 162-bis, 162-ter, 163, 164, 164-bis e 169), onde evitare la violazione del principio del "ne bis in idem". Sempre in tale ottica, in riferimento alle fattispecie penali più coincidenti con quelle integranti illeciti amministrativi (artt. 167, 167-bis e 167-ter) sono state introdotte particolari disposizioni finalizzate a coordinare il procedimento penale con quello amministrativo (commi 4, 5 e 6 dell'art. 167).

Quanto alle succitate fattispecie penali, trattasi di:

- "Trattamento illecito dei dati" (reclusione da sei mesi a tre anni, art. 167);
- "Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala" (reclusione da uno a sei anni, art 167-bis);
- "Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala" (reclusione da uno a quattro anni, art. 167-ter).

Tra gli altri illeciti penali sopravvissuti alla novella troviamo:

- "Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante" (art. 168);
- "Inosservanza di provvedimenti del Garante" (art. 170);
- "Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori" (art. 171).

Tra le fattispecie abrogate spicca l'art. 169, cui segue l'abrogazione del Capo I del Titolo V, parte I, del vecchio codice (Misure di sicurezza) e dell'allegato B, in ossequio alla disciplina dettata dal GDPR.

Ancora, l'art 24 del d.lgs. 101/2018 ("*Applicabilità delle sanzioni amministrative alle violazioni anteriormente commesse*") stabilisce che, per violazioni commesse anteriormente alla data di entrata in vigore del decreto, in luogo delle sanzioni penali precedentemente previste e oggi abrogate, troveranno applicazione le sostitutive sanzioni amministrative (purché il procedimento penale non sia stato definito con sentenza o con decreto divenuti irrevocabili). In tal caso, l'Autorità giudiziaria, entro novanta giorni dalla data di entrata in vigore del decreto, disporrà la trasmissione all'autorità amministrativa competente degli atti dei procedimenti penali relativi ai reati trasformati in illeciti amministrativi, salvo che il reato risulti prescritto o estinto per altra causa alla medesima data.

Infine, il decreto di adeguamento affida al Garante la definizione delle modalità del procedimento per l'adozione dei provvedimenti e delle sanzioni amministrative e i relativi termini (art. 166, comma 9, del novellato Codice Privacy), ferma restando l'applicazione de gli articoli da 1 a 9, da 18 a 22 e da 24 a 28 della legge 24 novembre 1981, n. 689, in quanto compatibili.

4. Politiche relative al trattamento dei dati

Nei paragrafi che seguono sono elencati e descritti i precetti e le direttive cui devono attenersi coloro che trattano i dati per conto del Titolare e/o sotto l'autorità dello stesso.

4.1 Principi generali del trattamento

Tutti i destinatari devono:

- rispettare i principi generali del Regolamento (UE) n. 2016/679 (cfr. par. 3.1.3), con particolare riferimento alla liceità e correttezza del proprio agire, all'obbligo di procedere alla raccolta e alla registrazione dei dati per scopi determinati, espliciti e legittimi;
- rispettare l'obbligo di riservatezza e segretezza e conseguentemente il divieto di comunicazione e diffusione dei dati trattati nel corso dell'incarico svolto;
- utilizzare i dati, cui abbia accesso, solamente per finalità compatibili all'esecuzione delle proprie mansioni o dei compiti affidati, per cui è autorizzato ad accedere alle informazioni e ad utilizzare gli strumenti lavorativi;
- rispettare le misure di sicurezza idonee adottate dalla società, atte a salvaguardare la riservatezza e l'integrità dei dati;
- segnalare eventuali malfunzionamenti di strumenti elettronici, perdite di dati o esigenze (sia di natura organizzativa, sia tecnica), che possano migliorare lo svolgimento delle operazioni affidate;
- accedere ai dati strettamente necessari all'esercizio delle proprie funzioni e competenze;
- in caso di interruzione del lavoro, anche temporanea, verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- mantenere riservate le proprie credenziali di autenticazione;
- svolgere le attività previste dai trattamenti secondo le direttive del responsabile del trattamento dei dati; non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento dei dati;
- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- informare il responsabile in caso di incidente di sicurezza che coinvolga dati particolari e non;
- raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli di studio e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
- eseguire qualsiasi altra operazione di trattamento nei limiti di quanto consentito e nel rispetto delle norme di legge.

Divieti generali

Di seguito sono riportati divieti validi per tutti i destinatari:

- alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
- accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
- accedere abusivamente al sistema informatico o telematico del Titolare al fine di alterare e /o cancellare dati e/o informazioni;
- detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al sistema informatico o telematico del Titolare o di soggetti concorrenti, pubblici o privati al fine di acquisire informazioni riservate;
- svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico di soggetti, pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;
- svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni;
- svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;
- svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
- caricare programmi non provenienti da una fonte certa e autorizzata dal Titolare;
- acquistare licenze software da una fonte (rivenditore o altro) non certificata e non in grado di fornire garanzie in merito all'originalità/autenticità del software;
- detenere supporti di memorizzazione di programmi non originali (DVD\CD\floppy);
- installare un numero di copie di ciascun programma ottenuto in licenza superiore alle copie autorizzate dalla licenza stessa, al fine di evitare di ricadere in possibili situazioni di *underlicensing*;
- utilizzare illegalmente password di computer, codici di accesso o informazioni simili per compiere una delle condotte sopra indicate;
- utilizzare strumenti o apparecchiature, inclusi programmi informatici, per decriptare software o altri dati informatici;

- distribuire i software del Titolare a soggetti terzi;
- realizzare codice software che violi copyright di terzi;
- accedere illegalmente e duplicare banche dati.

4.2 Accessi alle aree di lavoro e gestione delle postazioni

Accessi alle aree di lavoro

L'accesso agli uffici, alle aree protette, alle aree riservate ed agli archivi cartacei, è permesso ai soggetti espressamente autorizzati, in base a precise e motivate esigenze lavorative.

I visitatori e gli ospiti di vario genere (clienti, partner commerciali, fornitori e consulenti etc.) potranno avere accesso alle aree di lavoro esclusivamente previa autorizzazione.

È, pertanto, fondamentale che le aree di lavoro - ove sono custoditi i dati personali (ed in particolare quelli di natura sensibile) - siano soggette a controllo e a verifica, al fine di evitare che durante l'orario di lavoro i dati possano essere conosciuti o accessibili da parte di soggetti non autorizzati.

A livello fisico, tali controlli di sicurezza sono eseguiti tramite:

- procedure di identificazione e di autorizzazione all'accesso,
- sistema di allarme e di sorveglianza degli ambienti di lavoro,

A livello logico i controlli di sicurezza sono eseguiti tramite:

- procedure e sistemi di identificazione e riconoscimento dell'utente, (credenziali di autenticazione, etc.)
- sistema antintrusione, antivirus, con soluzioni tecnologicamente all'avanguardia.

Gli accessi fisici di terzi per le sole attività di servizio o di fornitura sono regolamentate dai contratti; mentre tutti gli accessi logici di terzi, se previsti, sono regolamentati da precisi accordi contrattuali che determinano i vincoli e le regole di accesso.

Le aree di lavoro sono protette da controlli di accesso tali da garantire che solo il personale autorizzato possa accedervi. Il personale esterno potrà accedervi solo previa autorizzazione e, in ogni caso, accompagnato da personale autorizzato.

Per il personale interno l'accesso è tenuto sotto controllo mediante:

- la sottoscrizione delle autorizzazioni al trattamento dei dati e eventuali accordi di riservatezza;

- il riconoscimento personale da parte delle altri autorizzati;

I visitatori e gli ospiti devono sostare esclusivamente nei locali individuati come "area attesa/reception".

Nei locali in cui avviene il trattamento dati possono accedere soltanto i soggetti autorizzati.

È affidato agli stessi autorizzati l'onere di controllare che nei locali non entrino altri soggetti che non abbiano l'appropriata autorizzazione.

Tutto il personale adotterà misure di identificazione a vista e deve essere esortato a chiedere il riconoscimento degli estranei non accompagnati.

Qualora dovessero accedere soggetti terzi nei locali in cui viene effettuato il trattamento dati, come ad esempio durante le operazioni di pulizia o manutenzione, è compito degli autorizzati sorvegliare l'operato dei soggetti non autorizzati, in modo che questi ultimi non possano comunque acquisire dati o informazioni, per osservazione diretta o altro metodo di cattura di dati o informazioni.

L'accesso agli archivi contenenti categorie particolari di dati (ex dati sensibili), o giudiziari, o comunque riservati, è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici, le persone che vi accedono devono essere sono preventivamente autorizzate.

Gestione delle postazioni

L'utilizzo della postazione di lavoro e il conseguente accesso ai documenti, atti e archivi è consentito nei limiti della propria funzione e dei propri incarichi.

La propria scrivania/postazione deve essere mantenuta in ordine, verificando di non lasciare documenti e atti riservati senza un proprio controllo all'accesso di terzi, in momenti di pausa, terminata la giornata di lavoro e/o in periodi di assenza.

In caso di allontanamento dal proprio ufficio o dalla propria postazione di lavoro, ciascun soggetto autorizzato allo svolgimento delle operazioni di trattamento deve adottare tutte le accortezze e precauzioni al fine di impedire l'accesso fisico a chi non sia legittimato, soprattutto se esterno o non specificamente autorizzato.

Qualora l'autorizzato utilizzi, nello svolgimento delle proprie mansioni, atti/documenti contenenti dati personali o sensibili, questi non devono essere lasciati incustoditi e occorre siano evitati eventuali accessi o la conoscenza da parte di soggetti non autorizzati; alla fine

del ciclo di lavoro, la documentazione deve essere SEMPRE riposta negli archivi ad accesso controllato.

4.3 Utilizzo delle risorse informatiche

Tutte le risorse informatiche messe a disposizione dei destinatari (di seguito anche utenti) dal Titolare devono essere utilizzate secondo le disposizioni contenute nei paragrafi seguenti.

4.3.1 Utilizzo dei PC

Il computer consegnato all'utente è uno strumento di lavoro e contiene tutti i software necessari a svolgere le attività affidate. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, rallentamenti del sistema, costi di manutenzione e, soprattutto, minacce alla sicurezza.

L'accesso all'elaboratore è protetto da credenziali di autenticazione (*user name* e password) che devono essere custodita dall'autorizzato con la massima diligenza e non divulgate (cfr. par. 4.3.3).

Per necessità lavorative del Titolare, gli amministratori di sistema, utilizzando la propria *login* con privilegi di amministratore e la password dell'amministratore, potranno accedere sia alle memorie di massa locali di rete (*repository* e backup) sia ai server del Titolare nonché, previa comunicazione al lavoratore, accedere al computer, anche in remoto.

Non è consentito all'autorizzato modificare le caratteristiche impostate sul proprio PC, salvo autorizzazione esplicita del Titolare o del Responsabile IT.

Colui che utilizza il PC:

- Se si allontana dalla propria postazione, dovrà mettere in protezione il suo dispositivo affinché persone non autorizzate non abbiano accesso ai dati protetti;
- Dovrà bloccare il suo dispositivo prima delle pause e, in generale, ogni qualvolta abbia bisogno di allontanarsi dalla propria postazione;
- Dovrà chiudere la sessione (*Logout*) a fine giornata;
- Dovrà spegnere il PC dopo il *Logout*;
- Dovrà controllare sempre che non vi siano persone non autorizzate alle sue spalle che possano prendere visione delle schermate del suo dispositivo;
- Dovrà mantenere sul computer esclusivamente i dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori), disposti dall'organizzazione;

- Non dovrà dare accesso al proprio computer ad altri utenti, a meno che siano altri autorizzati con cui condividono l'utilizzo dello stesso Pc o a meno di necessità stringenti e sotto il proprio costante controllo.

Deve sempre essere attivato lo *screen saver* e l'accesso con credenziali.

In ogni caso lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il Responsabile dei sistemi informatici nel caso in cui vengano rilevati virus.

4.3.2 Utilizzo di *Notebook*, *Tablet*, *Smartphone* etc.

Il computer portatile (*notebook*), il *tablet* e lo *smartphone* (di seguito generalizzati in "dispositivi mobili") possono venire concessi in uso dal Titolare agli utenti che durante gli spostamenti necessitino di disporre di archivi elettronici, supporti di automazione e/o di connessione alla rete.

L'utente è responsabile dei dispositivi mobili assegnatigli e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai dispositivi mobili si applicano le regole di utilizzo previste per i computer connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

I file creati o modificati sui dispositivi mobili, devono essere trasferiti sulle memorie di massa del Titolare al primo rientro in ufficio e cancellati in modo definitivo dai dispositivi mobili (*Wiping*).

Sui dispositivi mobili è vietato installare applicazioni (anche gratuite) se non espressamente autorizzate. I dispositivi mobili utilizzati all'esterno (convegni, eventi, sopralluoghi ecc…), in caso di allontanamento, devono essere custoditi in un luogo protetto.

In caso di perdita o furto dei dispositivi mobili, deve far seguito la denuncia alle autorità competenti. Allo scopo, si deve immediatamente avvisare il Titolare che provvederà – se del caso – ad occuparsi delle procedure connesse al *data breach*. Anche di giorno, durante l'orario di lavoro, all'utente non è consentito lasciare incustoditi i dispositivi mobili.

All'utente è vietato lasciare i dispositivi mobili incustoditi e a vista dentro l'auto o in una stanza d'albergo o nell'atrio dell'albergo o nelle sale d'attesa delle stazioni ferroviarie e aeroportuali.

I dispositivi mobili che permettono l'attivazione di una procedura di protezione (PIN) devono sempre essere abilitabili solo con la digitazione del PIN stesso e non possono essere lasciti privi di PIN.

Laddove il dispositivo mobile sia accompagnato da un'utenza, l'utente è chiamato ad informarsi preventivamente dei vincoli ad essa associati (es. numero minuti massimo, totale gigabyte, dati) e a rispettarli. Qualora esigenze lavorative richiedessero vincoli differenti, l'utente è tenuto ad informare tempestivamente e preventivamente il Titolare.

In relazione alle utenze mobili, salvo autorizzazione del Titolare, è espressamente vietato ogni utilizzo all'estero.

4.3.3 Credenziali di autenticazione

Le credenziali, composte da autorizza sono un metodo di autenticazione adottato dal Titolare per garantire l'accesso protetto ad uno strumento hardware, oppure ad un applicativo software.

Le credenziali di ingresso alla rete e di accesso ai programmi sono previste ed attribuite dal Titolare o dal Responsabile IT.

La prima caratteristica di una password è la segretezza: essa, pertanto, non deve essere svelata ad altri soggetti. La divulgazione delle proprie password o la trascuratezza nella loro conservazione può causare gravi danni al proprio lavoro, a quello dei colleghi e al Titolare nel suo complesso. Nel tempo, anche la password più sicura perde la sua segretezza. Per questo motivo è buona norma cambiarle con una certa frequenza.

A tal proposito, è necessario procedere alla modifica della password a cura dell'autorizzato del trattamento al primo utilizzo e, successivamente, almeno ogni sei mesi; nel caso di trattamento di categorie particolari di dati (ex dati sensibili) e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi con contestuale comunicazione al Responsabile dei sistemi informatici (n.b.: in molti sistemi la comunicazione di variazione può essere "generata" dallo stesso sistema informatico all'atto della modifica, con invio di e-mail automatica all'utilizzatore; molti sistemi permettono di "temporizzare" la validità delle password e, quindi, di bloccare l'accesso al personale computer e/o al sistema, qualora non venga autonomamente variata dall'autorizzato entro i termini massimi).

Al fine di favorire la corretta gestione delle password, devono essere adottate le seguenti regole:

- Le password devono essere composte da almeno otto caratteri e contenere almeno una lettera maiuscola (ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema), un numero e un carattere speciale (es.: { } [ ], . < > ; : ! " £ $ % & / ( ) = ? ^ \ | ' * - + _. ;);
- Le password sono assolutamente personali e non vanno mai comunicate ad altri;
- Le password devono essere sostituite almeno nei tempi suindicati, a prescindere dall'esistenza di un sistema automatico di richiesta di aggiornamento password.
- La password deve essere immediatamente sostituita, dandone comunicazione al Titolare o al Responsabile IT, nel caso in cui si sospetti che la stessa abbia perso la segretezza.
- Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia al Titolare o al Responsabile IT.

Ancora, è fatto espressamente divieto di:

- memorizzare password su alcun tipo di supporto, quali, ad esempio, Post-It (sul monitor o sotto la tastiera) o agende (cartacee e posta elettronica) o telefono cellulare.
- comunicare a chiunque altro le proprie credenziali di accesso al sistema informatico;
- utilizzare password:
  - corrispondenti a nome, cognome o loro parti;
  - corrispondenti allo user name;
  - corrispondenti all'indirizzo di posta elettronica (e-mail);
  - corrispondenti a parole comuni (in Inglese e in Italiano);
  - corrispondenti a date, mesi dell'anno e giorni della settimana, anche in lingua straniera;
  - corrispondenti a parole banali e/o di facile intuizione (ad es. "*qwerty*", "*12345678*" "*password", "security"* e palindromi);
  - corrispondenti a ripetizioni di sequenze di caratteri (es. *abcabcabc*);
  - corrispondenti a password già impiegata in precedenza;
  - contenenti riferimenti agevolmente riconducibili all'utilizzatore (data di nascita, numeri di telefono, targa dell'auto, nome di mogli/mariti/partner/figli etc.).

Inoltre, è buona norma evitare di digitare la propria password in presenza di altri soggetti che possano vedere la tastiera, anche se collaboratori o dipendenti del Titolare.

Accesso o *Login*

Il "*Login*" è l'operazione con la quale l'utente si connette al sistema informativo o ad una parte di esso, dichiarando il proprio *User name* e Password, aprendo una sessione di lavoro. In molti casi è necessario effettuare più login, tanti quanti sono gli ambienti di lavoro (ad es. applicativi web, Intranet, etc.), ognuno dei quali richiede uno username e una password.

Il "*Logout*" è l'operazione con cui viene chiusa la sessione di lavoro. Al termine della giornata lavorativa, tutte le applicazioni devono essere chiuse secondo le regole previste dall'applicazione stessa. La non corretta chiusura può provocare una perdita di dati o l'accesso agli stessi da parte di persone non autorizzate.

Il "*blocco del computer*" è l'operazione con cui viene impedito l'accesso alla sessione di lavoro (tastiera e schermo disattivati) senza chiuderla.

In alcuni casi, sono implementati meccanismi che consentono all'utente un numero limitato di tentativi errati di inserimento della password, oltre ai quali il tentativo di accesso viene considerato un attacco al sistema e l'account viene bloccato per alcuni minuti. In caso di necessità, contattare il Titolare o il Responsabile IT.

Controllo e custodia delle credenziali

Nell'ambito delle attività riguardanti la tutela della sicurezza dell'infrastruttura tecnologica, il Titolare potrebbe effettuare analisi periodiche sulle credenziali degli utenti al fine di verificarne la solidità, le policy di gestione e la durata, informandone preventivamente gli utenti stessi.

Nel caso in cui la verifica abbia, tra gli esiti possibili, la decodifica della password, questa viene bloccata e richiesto al Responsabile IT di cambiarla.

Il Titolare e/o il soggetto da lui all'uopo individuato hanno la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica interna ed esterna. A tale scopo, detengono copia delle credenziali di autenticazione di ciascun utente.

Il Titolare e/o il soggetto da lui all'uopo individuato potranno accedere ai dati ed agli strumenti informatici esclusivamente al fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività lavorativa nei casi in cui si renda indispensabile ed indifferibile l'intervento (ad esempio, in caso di prolungata assenza o impedimento dell'autorizzato, informando tempestivamente l'autorizzato dell'intervento di accesso realizzato).

Perdita delle condizioni

Le password che non vengono utilizzate da parte dei responsabili per un periodo superiore ai sei mesi, verranno disattivate.

In qualsiasi momento, il Titolare si riserva il diritto di revocare all'utente il permesso di accedere ad un sistema hardware o software a cui era precedentemente autorizzato, rimuovendo user name o modificando/cancellando la password ad esso associata.

4.3.4 Utilizzo dei dispositivi e supporti removibili

Nell'ambito delle attività lavorative, il personale può essere dotato di dispositivi rimovibili messi a disposizione dal Titolare (hard disk portatili, chiavette USB, DVD ecc.). Tali dispositivi devono, essere connessi o utilizzati esclusivamente su computer di lavoro.

Se non diversamente stabilito e regolamentato da apposita procedura operativa, è tassativamente vietato trasferire, anche solo temporaneamente, copie di categorie particolari di dati personali (sensibili: es. dati sanitari degli assistiti) su qualsiasi dispositivo rimovibile. Nel caso in cui vi sia la necessità di memorizzare su dispositivi rimovibili tali dati, l'utilizzo in deroga al divieto deve essere autorizzato dal Titolare e l'archiviazione deve avvenire in modo cifrato, usando algoritmi di crittografia sufficientemente robusti ed affidabili, riconosciuti come standard internazionali.

I dispositivi e i supporti contenenti categorie particolari di dati personali devono essere custoditi in archivi chiusi a chiave.

In caso di riutilizzo/dismissione dei supporti, l'utente deve assicurarsi che si proceda, prima dello smaltimento, all'eliminazione permanente delle informazioni e dei dati memorizzati affinché questi non possano essere in alcun modo recuperati.

4.3.5 Utilizzo della rete

Il personale autorizzato deve utilizzare le risorse di rete a disposizione (ad es: internet, intranet) in maniera responsabile e al solo scopo di espletare le proprie attività lavorative, evitando comportamenti e modalità di utilizzo che possono causare oltre che una perdita di produttività, anche rischi per l'integrità, la riservatezza e la disponibilità delle informazioni.

Un utilizzo improprio di tali risorse può portare alla sospensione dell'account ed essere soggetto ad eventuali procedimenti disciplinari e/o azioni legali.

In particolare, il personale esterno che opera presso la struttura non può connettersi alla rete con il proprio portatile se non previa esplicita autorizzazione del Titolare.

Rete locale:

La rete locale (intranet) è utilizzata per la condivisione di informazioni strettamente legate alle attività lavorative e non deve essere utilizzata per finalità differenti.

Le unità di rete sono aree di condivisione di informazioni professionali e non possono in alcun modo essere utilizzate per scopi diversi.

Qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità.

Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup. La corretta effettuazione dei backup è verificata dal Titolare, o da un soggetto dallo stesso designato, il quale verificherà la presenza di errori nei log di backup.

Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

Il Responsabile IT può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC sia sulle unità di rete.

Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.

Rete internet:

Il Titolare fornisce al personale autorizzato l'accesso alla rete Internet, al fine di facilitare la conduzione delle proprie attività lavorative. È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

L'uso occasionale della rete Internet per motivi personali non deve interferire con le attività lavorative e con le direttive impartite dal Titolare per l'esecuzione delle prestazioni.

Pertanto, l'uso della rete Internet è consentito per scopi leciti e professionali, e deve essere fatto in maniera responsabile. In particolare, l'utente non deve utilizzare la rete Internet per:

- inviare o salvare dati o file coperti da proprietà intellettuale;
- utilizzare servizi di accesso remoto non autorizzati che permettono l'accesso alla rete locale del Titolare;
- utilizzare social network, se non espressamente autorizzati;
- partecipare a Forum non professionali e utilizzare *chat line* (esclusi gli strumenti autorizzati) anche mediante pseudonimi (o *nickname*);
- pubblicare sulle bacheche elettroniche (es: forum, blog, social network) materiale di natura oscena, blasfema, diffamatoria oltraggiosa o discriminatoria per sesso (ad es. materiale pedopornografico, ecc..), lingua, religione, razza, origine etnica, opinione o appartenenza sindacale o politica;
- pubblicare su Social Network, Blog, Forum, informazioni o materiale riconducibile al Titolare che possa causare un qualsiasi danno allo stesso o a terzi;
- effettuare operazioni di registrazione a siti non attinenti alle attività lavorative;
- navigare nei siti che possono rivelare le opinioni politiche religiose, sindacali e di salute dell'utente poiché potenzialmente idonea a rivelare categorie particolari di dati;

- accedere a siti internet che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico, rilevante ai fini della realizzazione di una fattispecie di reato o che siano in qualche modo discriminatori sulla base della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap;
- copiare e distribuire materiale coperto da diritto d'autore;
- causare o tentare di violare le misure di sicurezza di altre organizzazioni;
- utilizzare la rete per violare le vigenti leggi dello Stato italiano o di qualunque altro Stato;
- memorizzare documenti informatici di natura oltraggiosa, diffamatoria e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- promuovere utile o guadagno personale attraverso l'uso di Internet o della posta elettronica lavorativa;
- creare siti web personali sui sistemi dell'organizzazione;
- effettuare ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dal Titolare e con il rispetto delle normali procedure di acquisto;

L'utente è pertanto responsabile sia disciplinarmente che giuridicamente, dei danni arrecati attraverso l'uso privato, improprio o illecito della connessione ad internet.

Il Titolare potrà adottare idonee misure tecniche preventive volte a ridurre navigazioni a siti non correlati all'attività lavorativa attraverso filtri e black list.

Accesso da remoto (VPN - VIRTUAL PRIVATE NETWORK)

L'accesso dall'esterno alla rete del Titolare è consentito esclusivamente attraverso precise modalità di connessione sicura indicate dal Titolare stesso.

Ogni altro accesso è espressamente vietato.

4.3.6 Utilizzo della posta elettronica

La casella di posta, assegnata dal Titolare all'autorizzato, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

È fatto divieto di utilizzare le caselle di posta elettronica messa a disposizione dal Titolare per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing list salvo diversa ed esplicita autorizzazione.

Gli indirizzi di posta elettronica possono essere nominativi (es. "*m.rossi@...")* o assegnate con natura impersonale (tipo *info*, *amministrazione*, *fornitori*, *privacy*, *job*, *etc*.) proprio per evitare ulteriormente che il destinatario delle mail possa considerare l'indirizzo assegnato all'utente come "privato".

La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

Le e-mail inviate devono necessariamente contenere il *disclaimer* predisposto dal Titolare.

Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali deve essere visionata o autorizzata dal Titolare, o in ogni modo è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.

La documentazione elettronica che costituisce per il titolare "*know how*" tecnico o commerciale protetto, e che, quindi, viene contraddistinta da diciture o avvertenze dirette ad evidenziarne il carattere riservato o segreto a tutela del patrimonio, non può essere comunicata all'esterno senza preventiva autorizzazione del Titolare.

È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti tradizionali (PEC, fax, raccomandate A/R).

È obbligatorio controllare i file *attachments* di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

È vietato:

- inviare, tramite la posta elettronica materiale a contenuto violento, sessuale o comunque offensivo dei principi di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazione del pensiero, anche politico.
- inviare messaggi di posta elettronica che abbiano contenuti contrari a norme di legge ed a norme di tutela dell'ordine pubblico, rilevanti ai fini della realizzazione di una fattispecie di reato, o che siano in qualche modo discriminatori della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.
- utilizzare l'indirizzo di posta elettronica contenente il nome di dominio del Titolare per iscriversi in qualsivoglia sito per motivi non attinenti all'attività lavorativa, senza espressa autorizzazione scritta, nonché utilizzare tale dominio per scopi personali.

- creare, archiviare o spedire messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) non connessi con lo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto, "catene di Sant'Antonio" o in genere a pubblici dibattiti utilizzando l'indirizzo lavorativo;
- sollecitare donazioni di beneficenza, propaganda elettorale o altre voci non legate al lavoro;
- utilizzare il servizio di posta elettronica per trasmettere a soggetti esterni dell'organizzazione informazioni riservate o comunque documenti lavorativi, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte;
- utilizzare la posta elettronica per messaggi con allegati di grandi dimensioni.

Posta Elettronica in caso di assenze programmate ed assenze non programmate

Nel caso di assenza prolungata sarebbe buona norma attivare il servizio di risposta automatica (*auto-reply*).

In alternativa, e in tutti i casi in cui sia necessario un presidio della casella di e-mail per ragioni di operatività lavorativa, l'utente deve nominare un collega che in caso di assenza inoltri i file necessari a chi ne abbia urgenza.

Qualora l'utente non abbia provveduto ad individuare un collega fiduciario o questi sia assente o irreperibile, il Titolare, mediante personale appositamente individuato, potrà verificare il contenuto dei messaggi di posta elettronica dell'utente, informandone lo stesso e redigendo apposito verbale.

Disattivazione dell'account di posta di tipo individualizzato

nometitolare, in conformità ai principi in materia di protezione dei dati personali, dopo una eventuale cessazione del rapporto di lavoro rimuoverà gli account di posta elettronica aziendali riconducibili a persone identificate o identificabili, in un tempo ragionevole commisurato ai tempi tecnici di predisposizione delle misure.

La rimozione dell'account individualizzato avverrà mediante:

- disattivazione dello stesso ad opera della funzione di Information Technology;
- adozione di sistemi automatici volti ad informarne i terzi ed a fornire a questi ultimi indirizzi alternativi riferiti all'attività professionale del titolare del trattamento.

Si provvederà altresì ad adottare misure idonee ad impedire la visualizzazione dei messaggi in arrivo durante il periodo in cui tale sistema automatico è in funzione.

Lo scopo di tali misure tecnologiche ed organizzative è di contemperare l'interesse del titolare ad accedere alle informazioni necessarie all'efficiente gestione della propria attività

e a garantirne la continuità con la legittima aspettativa di riservatezza sulla corrispondenza da parte di dipendenti/collaboratori nonché dei terzi.

4.3.7 Installazione di hardware e software

L'installazione di hardware e software, nonché la modifica dei parametri di configurazione, possono essere eseguiti solamente dalle persone del Servizio Informatico su mandato del Titolare del trattamento. Pertanto, gli utenti devono attenersi ai seguenti divieti:

- Non installare e utilizzare sul PC dispositivi personali, o comunque non autorizzati dal Titolare (come ad esempio masterizzatori, modem, dispositivi di memorizzazione dei dati ecc.), se non con l'approvazione espressa del Titolare;
- Non installare sistemi per connessione esterne (es: modem, wifi); tali connessioni, aggirando i sistemi preposti alla sicurezza della rete, aumentano sensibilmente i rischi di intrusioni e di attacchi dall'esterno;
- Non installare e utilizzare programmi, anche in versione demo. In particolare, è vietata l'installazione di giochi, programmi in prova (shareware), programmi gratuiti (freeware), programmi pirata, e in generale tutti i software non autorizzati dal Titolare;
- Più in generale, non utilizzare programmi diversi da quelli distribuiti ed installati ufficialmente dal Titolare o del Responsabile IT;
- Non modificare i parametri di configurazione del proprio PC senza espressa autorizzazione e senza il supporto di personale tecnico qualificato;

Si ricorda che normalmente la condivisione di aree e di risorse del proprio PC è vietata. Può essere autorizzata dal Titolare, solo in casi eccezionali e solo per il tempo strettamente necessario allo svolgimento delle attività di lavoro. In questi casi devono essere adottate password di lettura e scrittura e la condivisione deve operare solo su singole directory del PC, e non sull'intero disco rigido.

L'inosservanza delle disposizioni su elencate, oltre al rischio di danneggiamenti del sistema per incompatibilità con hardware e software esistente, può esporre il Titolare a gravi responsabilità civili ed anche penali; in particolare, in caso di violazione della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato.

I controlli sui software operativi sono di due tipologie, quelli inerenti i sistemi operativi e quelli relativi ai *tools* di sviluppo o applicazioni.

Nel primo caso, sarà compito dell'amministratore di sistema dotare sia i server che i client di sistemi operativi aggiornati o utili agli scopi desiderati preoccupandosi di rintracciare le necessarie patch utili a proteggere tali sistemi da incursioni esterne.

Nel secondo caso, sarà premura del Titolare verificare che le versioni degli applicativi in uso siano compatibili con i sistemi operativi presenti ed aggiornati periodicamente.

ANTIVIRUS

I virus (*malware*) possono essere trasmessi tramite scambio di file via internet, via mail, scambio di supporti removibili, filesharing, chat, etc..

Per prevenire eventuali danneggiamenti al software causati dalla presenza o dall'azione di virus informatici, su ogni elaboratore messo a disposizione dal Titolare è stato installato un software antivirus che deve essere aggiornato all'ultima versione disponibile.

Gli aggiornamenti del programma forniscono miglioramenti al prodotto software installato.

Qualora non siano adottati o correttamente funzionanti sistemi automatici di aggiornamento dei sistemi antivirus, gli utenti devono procedere all'effettuazione delle operazioni di aggiornamento, di volta in volta richieste dal sistema, secondo le istruzioni visualizzate sullo schermo.

Giornalmente il sistema antivirus esegue, se lo ritiene necessario, *l'update* della banca dati dei virus senza richiedere l'intervento dell'utente scaricando il nuovo file delle definizioni ed aggiornamenti software attraverso il collegamento Internet.

L'antivirus installato dal Titolare non deve mai essere disattivato o sostituito con altro antivirus non ufficialmente fornito.

Nel caso il programma antivirus installato sul proprio PC riscontri la presenza di un virus, oppure si sospetti la presenza di un virus non rilevato dal programma antivirus è necessario darne immediatamente segnalazione al responsabile del Servizio Informatico o, in mancanza, direttamente al Titolare. Successivamente, si procederà immediatamente a:

- isolare il sistema dalla rete informatica;
- verificare se ci sono altri sistemi infettati con lo stesso virus informatico;
- identificare l'antivirus o le patch adatte a bonificare il sistema infetto;
- installare l'antivirus o la patch adatta su tutti gli altri sistemi che ne sono sprovvisti;

Si raccomanda di non scaricare e né tantomeno aprire file provenienti via e-mail da mittenti sconosciuti. Tali file, possono essere portatori di virus e compromettere la funzionalità del PC, l'integrità dei dati in essa contenuti e soprattutto l'integrità dei sistemi collegati al PC stesso.

Il software Antivirus deve essere configurato con le seguenti caratteristiche:

- Caricamento all'avvio del computer (funzione *Auto-Protect*);
- Attivazione scansione e-mail in entrata ed in uscita;
- Scansione intero sistema;
- Attivazione blocco degli script;
- Aggiornamento automatico;
- Per i file in entrata automatica prevedere la cancellazione del file infetto.

Ogni utente deve inoltre attenersi alle seguenti regole:

- È vietato accedere alla rete senza servizio antivirus attivo e aggiornato sulla propria postazione.
- È vietato ostacolare l'azione dell'antivirus.
- È vietato disattivare l'antivirus senza l'autorizzazione espressa dell'Istituto, anche e soprattutto nel caso sia richiesto per l'installazione di software sul computer.
- È vietato aprire allegati di mail provenienti da mittenti sconosciuti o di dubbia provenienza o allegati di mail di persone conosciute ma con testi inspiegabili o in qualche modo strani.

Contattare i sistemi informativi prima di procedere a qualsiasi attività potenzialmente in conflitto con quanto sopra.

4.3.8 Amministratori di sistema

Sono individuati dal Titolare lo/gli Amministratore/i di Sistema.

All'Amministratore di Sistema è assegnata l'attività di gestione tecnica del sistema informatico finalizzata alla sicurezza del trattamento dei dati mediante strumenti elettronici.

Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, sono riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti da parte dell'Autorità Garante.

Qualora sia necessario individuare un Amministratore di sistema esterno, l'elenco dei nominativi dei soggetti preposti alle specifiche funzioni deve essere comunicato dalle Ditte esterne al Titolare, ai fini della predisposizione della documentazione necessaria alla loro individuazione in qualità di amministratori di sistema.

Sono affidati all'Amministratore di sistema i seguenti compiti:

- gestire le credenziali di autenticazione dei soggetti autorizzati al trattamento/addetti alla manutenzione;
- gestire i profili di autorizzazione degli autorizzati al trattamento dei dati/addetti alla manutenzione, su specifiche indicazioni impartite dal Titolare del trattamento;
- provvedere alla disattivazione/variazione delle utenze assegnate al personale cessato dal servizio o che abbia modificato il proprio ambito di trattamento, su richiesta specifica del titolare;
- custodire la documentazione cartacea, prodotta nello svolgimento dei propri compiti;
- adottare i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al loro ricovero periodico con copie di back-up secondo i criteri stabiliti;
- assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro;
- prevedere procedure operative per la disattivazione delle credenziali di accesso, in caso di perdita della qualità di autorizzato all'accesso all'elaboratore, oppure nel caso di mancato utilizzo delle credenziali per un periodo superiore a 6 mesi;
- proteggere gli strumenti elettronici dal rischio di intrusione (violazione del sistema da parte di "hacker") e dal rischio di programmi virus mediante idonee misure di sicurezza;
- mantenere un adeguato sistema di autorizzazione che, per ogni identificativo utente, riporti la data di attivazione, le funzioni del sistema alle quali l'utente è abilitato, la data di cessazione dell'identificativo stesso;
- provvedere al salvataggio dei dati presenti sui server e al loro ripristino in caso di necessità;
- conservare le copie di back-up;
- registrare e archiviare tutte le attività eseguite sul sistema (log);
- garantire che le informazioni scambiate con soggetti interni ed esterni siano opportunamente protette da rischi di intrusione.

4.3.9 Manutenzione

Il Titolare, ove necessario, ricorre ad addetti alla manutenzione ai quali possono essere affidate le seguenti attività:

- effettuare operazioni di manutenzione e supporto per la verifica del corretto funzionamento (monitoraggio e diagnostica) su flussi dei dati;
- effettuare operazioni di manutenzione e supporto per la verifica del corretto funzionamento dei computer, dispositivi mobili, posta elettronica, software, etc.;
- gestire le credenziali di autenticazione dei soggetti autorizzati su indicazione dell'Amministratore di sistema o del Titolare;
- gestire i profili di autorizzazione degli autorizzati al trattamento dei dati, su specifiche impartite dal Titolare o su indicazione dell'Amministratore di sistema;
- provvedere alla disattivazione/variazione delle utenze, ivi compreso l'account di posta elettronica, assegnate al personale cessato dal servizio o che abbia modificato il proprio ambito di trattamento, su richiesta specifica del Titolare e su indicazione dell'Amministratore di sistema;
- custodire la documentazione cartacea, prodotta nello svolgimento dei propri compiti;

L'accesso agli addetti alla gestione e manutenzione è consentito unicamente ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere alle operazioni di manutenzione dei programmi o del sistema informatico.

A ciascun addetto alla manutenzione è pertanto consentito eseguire le operazioni strettamente necessarie a tali scopi e/o richieste dal titolare, secondo le seguenti istruzioni operative:

- nel caso in cui sia necessario effettuare stampe di prova per controllare il funzionamento di stampanti o per verificare il funzionamento di strumenti o programmi installati, non utilizzare file già esistenti ma creare file di prova;
- nel caso si renda strettamente necessario accedere a file contenenti dati (ad esempio per il recupero di un testo) limitare l'accesso ai dati per il tempo strettamente necessario all'assolvimento delle operazioni di manutenzione;
- per effettuare operazioni di manutenzione sui database lavorativi che prevedano la raccolta e la conservazione dei dati, tali dati dovranno essere custoditi in modo tale da non essere accessibili da soggetti non autorizzati;
- devono inoltre essere adottate le misure di sicurezza previste dalla normativa in materia di protezione dei dati personali;

- è necessario informare al più presto il titolare del trattamento qualora si dovessero riscontrare malfunzionamenti o non conformità;
- nel caso in cui sia necessario accedere ai dati attraverso gli strumenti elettronici in dotazione agli autorizzati, attenersi alle seguenti indicazioni:
  - in presenza dell'autorizzato, far digitare la password allo stesso evitando di venirne a conoscenza;
  - in assenza dell'autorizzato, rivolgersi alla persona individuata dallo stesso quale proprio fiduciario il quale provvederà all'inserimento della password;
- nei casi in cui sia necessario accedere ai dati personali attraverso il server, rivolgersi all'amministratore di sistema o provvedere, in collaborazione con l'amministratore di sistema stesso, alla creazione di credenziali di autenticazione da utilizzarsi esclusivamente per l'accesso da parte degli addetti alla manutenzione/gestione dei sistemi informatici;
- l'amministratore di sistema ha facoltà, in qualunque momento di controllare e verificare l'operato degli addetti alla manutenzione;
- qualora si renda necessario prelevare apparecchiature elettroniche per effettuare attività di ripristino o interventi di manutenzione che comportino il reset di password precedentemente individuate, la nuova password di accesso sarà comunicata all'incaricato il quale provvederà a cambiarla al termine delle operazioni di manutenzione;
- l'accesso al sistema informatico da parte degli addetti alla manutenzione/gestione del sistema è consentito unicamente previo inserimento di password e ID.

4.4 Archivi cartacei

Le politiche di utilizzo adottate dal Titolare in merito all'accesso e al trattamento degli archivi cartacei, con particolare riferimento ai documenti cartacei che riconducono a categorie particolari di dati personali, sono orientate a fornire requisiti di riservatezza, integrità e disponibilità equivalenti a quanto disposto per le informazioni trattate con strumenti informatici.

Per archivio si intende complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto durante lo svolgimento dell'attività.

Di seguito sono definite le regole minime che costituiscono la base di accesso ed utilizzo delle informazioni cartacee.

4.4.1 Accesso agli archivi cartacei

L'accesso agli archivi cartacei è permesso al solo personale autorizzato, in particolar modo per quanto riguarda l'accesso alle informazioni personali afferenti la persona fisica. Le autorizzazioni sono da ritenersi strettamente personali e non possono essere trasferite a terzi.

4.4.2 Protezione degli archivi cartacei

La protezione degli archivi cartacei è affidata a idonee misure di sicurezza fisica quali:

- Controllo degli accessi ai locali;
- Sistemi di archiviazione segregati, secondo criteri di aggregazione dei supporti cartacei con analoghi livelli di sensibilità;
- Tracciamento degli accessi effettuati.

Le misure di sicurezza adottate si applicano sia ai documenti originali che alle loro copie.

Gli autorizzati sono responsabili del controllo e della custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Gli autorizzati devono attenersi alle seguenti disposizioni:

- evitare di effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal titolare, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento; il numero di copie di documenti contenenti Dati Personali deve essere strettamente funzionale alle esigenze di lavoro;
- evitare di sottrarre, cancellare, distruggere senza l'autorizzazione del titolare stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento;
- evitare di consegnare a persone non autorizzate dal Titolare dei dati personali, stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento
- evitare il deposito di documenti di qualsiasi genere negli ambienti di transito o pubblici (corridoi o sale riunioni)
- in nessun caso accedere a documentazione contenente Dati Personali per motivi non dettati da esigenze di lavoro strettamente connesse ai trattamenti dichiarati, autorizzati e tutelati dal Titolare;
- archiviare i documenti in ambiente ad accesso controllato;

- fuori dall'orario di lavoro, chiudere a chiave cassetti ed armadi contenenti documentazione riservata
- prima di lasciare la propria postazione (per esempio per la pausa pranzo o per una riunione), riporre in luogo sicuro (armadio, cassettiera, archivio, …) i dati cartacei, affinché gli stessi non possano essere visti da terzi non autorizzati (es. addetti alle pulizie) o da terzi (visitatori);
- archiviare i documenti contenenti categorie particolari di dati personali in cassetti ed armadi chiusi a chiave
- quando gli atti e i documenti contenenti dati personali, dati particolari (ex dati sensibili) o giudiziari sono affidati agli Incaricati per lo svolgimento dei relativi compiti, controllare e custodire i medesimi atti e documenti fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e restituire al termine delle operazioni affidate;
- in nessun caso utilizzare documenti contenenti dati personali, categorie particolari di dati (ex dati sensibili) o giudiziari come carta da riciclo o da appunti.
- ove possibile, effettuare la scansione dei documenti cartacei ed archiviarli digitalmente.
- non lasciare incustoditi in un ambiente non controllato (ad es. a seguito della stampa dei documenti su stampante di rete) i documenti contenenti dati personali;
- rimuovere al termine dell'orario di lavoro la documentazione contenente Dati Personali che, per ragioni di praticità operativa, risiede sulle scrivanie.

Qualora i dati personali risiedano solo su documenti cartacei, è necessario effettuare le copie degli stessi, possibilmente in formato digitale.

Pertanto, è compito degli autorizzati:

- Prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di sicurezza secondo i criteri stabiliti dal titolare del trattamento.
- Assicurarsi della qualità delle copie di sicurezza dei dati.
- Assicurarsi della conservazione delle copie di sicurezza in luogo adatto e sicuro e ad accesso controllato.
- Provvedere a conservare con la massima cura e custodia i dispositivi utilizzati per le copie di sicurezza, impedendo l'accesso agli stessi dispositivi da parte di personale non autorizzato.

- Segnalare tempestivamente al Titolare ogni eventuale problema dovesse verificarsi nella normale attività di copia.

4.4.3 Smaltimento degli archivi cartacei

Lo smaltimento dei documenti cartacei contenenti dati personali deve avvenire nel pieno rispetto della normativa in materia di privacy.

In particolare, i documenti contenti categorie particolari di dati e/o dati giudiziari devono essere smaltiti osservando le seguenti modalità, salvo l'applicazione di ulteriori norme restrittive stabilite dal Titolare, per particolari tipologie di informazioni e/o trattamenti:

- ogni ufficio disporrà di un numero congruo di trita documenti;
- si procederà alla distruzione di documenti contenenti categorie particolari di dati personali attraverso tali appositi trita documenti;
- ove necessario, con apposto contratto di nomina di Responsabile Esterno, l'eventuale ditta incaricata del Servizio di Pulizia curerà la distruzione di documenti cartacei per i quali non si è provveduto alla distruzione con gli appositi strumenti;
- ove non siano disponibili strumenti per la distruzione dei documenti (trita documenti), o il volume di questi sia tale da imporre il ricorso al servizio di macero, il personale Autorizzato che avvia al macero la documentazione è tenuto a confezionare tale documentazione in modo che il pacco risulti anonimo e solido;
- saranno tracciati i trasporti del materiale cartaceo dagli archivi ai siti preposti alla distruzione e conservati i verbali di avvenuta distruzione;

Le modalità di esecuzione ed i requisiti di sicurezza applicabili alle procedure di smaltimento da parte di fornitori esterni devono essere definite a livello contrattuale ai sensi dell'art. 28 del Regolamento UE n. 2016/679.

4.6 Formazione e informazione

Allo scopo di adeguare le attività di trattamento svolte dal Titolare alle disposizioni di legge, viene effettuata regolare formazione in materia di privacy.

All'atto di sottoscrizione del contratto di lavoro o dell'incarico professionale, oltre a rendere note:

- le attività o le mansioni da assolvere,
- le procedure e regole di lavoro interne,

- gli obiettivi e l'influenza determinante che gli stessi hanno sulla qualità e sulla sicurezza delle informazioni interna ed esterna,

viene sottoscritto l'accordo di riservatezza e l'incarico per il trattamento dei dati personali in riferimento a quanto disposto dal GDPR.

Tutti i dipendenti e i terzi (quali collaboratori esterni), sono addestrati sulle procedure e informati sulle politiche del Titolare della sicurezza, tramite precise attività di formazione e di addestramento, così come previsto:

- dal Piano Annuale di formazione
- dai programmi specifici eseguiti in maniera straordinaria, per azioni di miglioramento o di correzione delle attività svolte,
- a fronte di modifiche a procedure o a politiche della sicurezza.

La formazione e l'addestramento possono essere realizzati per mezzo di insegnamenti diretti o per mezzo di corsi/seminari di formazione esterni.

Da un punto di vista del contenuto, si distinguono:

- Formazione sulle tematiche generali della privacy e della Sicurezza dei dati, effettuate dal Titolare o da personale esterno.
- Formazione specifica su privacy e sicurezza dei dati effettuata da personale esterno qualificato.
- Formazione professionale relativa agli aspetti specifici della professionalità delle singole funzioni.
- Addestramento tecnico specifico necessario, in funzione della tipologia del servizio da erogare, del processo e degli strumenti utilizzati per lo svolgimento del lavoro, effettuata internamente o dal fornitore (per software). Tale addestramento viene attuato:
  - Attraverso la spiegazione delle procedure, la discussione di argomenti specifici e la discussione con gli operatori su eventuali reclami, suggerimenti del cliente;
  - Attraverso l'affiancamento, per un periodo opportuno, ad un operatore esperto;
  - Mediante seminari tenuti da personale interno o esterno qualificato.

Tutte le attività formative sono pianificate. Le attività di formazione e addestramento vanno registrate mediante apposito verbale.

Sono registrate anche le attività formative svolte all'esterno, allegando l'eventuale attestato di frequenza rilasciato. Le registrazioni delle attività di formazione e addestramento relative a ciascun soggetto devono essere effettuate solo in seguito alla verifica dell'efficacia dell'attività formativa, ossia attraverso la consegna attestato (per i

corsi che già prevedono una verifica dell'apprendimento) o validazione da parte del docente che si è occupato della formazione.

4.7 Responsabilità e sanzioni

È fatto obbligo a tutti i destinatari di osservare le disposizioni portate a conoscenza con il presente Regolamento.

Ogni soggetto, sia questo un dipendente o consulente esterno, che tratta le informazioni e/o interagisca con i sistemi informativi di proprietà della Titolare, o dati in uso alla stessa, deve utilizzare le risorse in maniera responsabile e diligente, in linea con quanto stabilito dalle normative di legge (artt. 2104 e 2105 c.c.) e in adempimento alle disposizioni impartite dal Titolare del trattamento dei dati personali.

Chiunque non rispetti il presente Regolamento potrà essere soggetto all'immediata sospensione dell'accesso agli strumenti informatici.

Inoltre, il mancato rispetto o la violazione del presente Regolamento è perseguibile con provvedimenti disciplinari e risarcitori, nonché con tutte le azioni civili e penali consentite.

Fermi restando i profili di responsabilità civile e penale previsti dalla normativa vigente, in relazione ai dipendenti del Titolare si precisa che il mancato rispetto del presente Regolamento costituisce un comportamento sanzionabile disciplinarmente in quanto grave violazione degli obblighi contrattualmente assunti, con conseguente applicabilità di sanzioni disciplinari (anche ai sensi del vigente C.C.N.L.).

5. Validità e revisione del regolamento

Il presente documento è valido a partire dalla sua adozione ed è sottoposto a revisione e aggiornamento ogniqualvolta dovesse essere necessario in virtù di variazioni organizzative e/o aggiornamenti normativi primari e secondari.

Ogni eventuale variazione sarà debitamente comunicata a tutti destinatari.