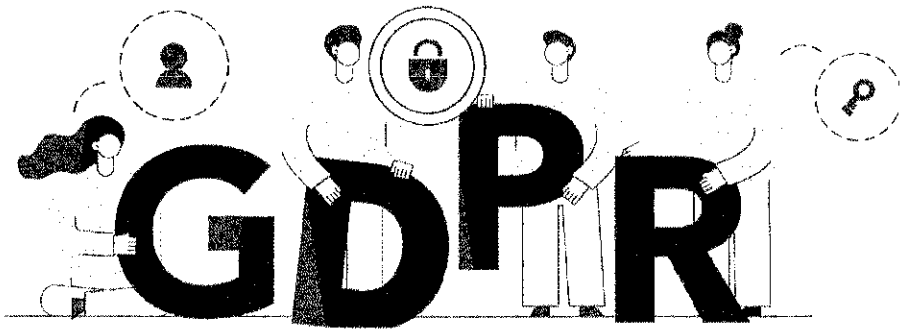
# MANUALE GDPR

*Ai sensi del Regolamento (UE)2016/679*




dell'azienda:

## Nigro Impianti S.r.l. con unico socio

Con riferimento alle seguenti Attività:

Installazione, manutenzione e riparazione di impianti elettrici civili ed industriali

Con riferimento alle seguenti Unità:

Sede Legale: Via Pacciarella - Contrada Bencivenga, 31, 70022, Altamura, (BA)

| *Titolare del Trattamento* | |
|---|---|
| *Redatto da:* | Nigro Impianti S.r.l. con unico socio |
| Approvato dal Rappresentante Legale<br>**Antonio Nigro** *(firma)* | NIGRO IMPIANTI SRL<br>Via Pacciarella, 31<br>70022 ALTAMURA (BA)<br>P.Iva: 07337360726 |
| *Data Creazione:* | 29/07/2015 |
| *Revisione e Data aggiornamento* | Revisione n° 2, in data 03/11/2023 |
| *Motivazione* | Monitoraggio, aggiornamento e verifica del 03/11/2023 |

**N.B.**: Con il termine **"Azienda"** si intende il Titolare del Trattamento la cui ragione sociale e dati anagrafici aziendali sono indicati in questa pagina.

# Allegati al Manuale GDPR

⇒ Organigramma Privacy

⇒ Contratti / Nomine GDPR

⇒ Verbale Formazione / Informazione GDPR

⇒ Informative GDPR

⇒ DPIA GDPR

⇒ Registro Titolare del trattamento GDPR

⇒ Modello di Notifica Garante (Data Breach)

⇒ Cartellone di videosorveglianza GDPR

⇒ Procedura per la gestione delle richieste di esercizio dei diritti degli interessati, artt. 15 - 22 del Regolamento UE 2016/679 (GDPR)

# Sommario

# 1 DISCIPLINARE

## 1.1 PREMESSA

Il 25 maggio 2016 è entrato in vigore, a livello di Comunità Europea, il **Nuovo Regolamento Europeo sulla Privacy** (*General Data Protection Regulation- GDPR*), con il quale la *Commissione Europea* intende rafforzare e armonizzare la protezione dei dati personali entro i confini dell'UE, sostituendo la direttiva sulla protezione dei dati 95/46/CE. Le Norme saranno applicabili a partire dal 25 maggio 2018.

Il Regolamento ha portato una serie di innovazioni, la **protezione dei dati passa da un approccio formale di adempimenti a un metodo più sostanziale**, con lo scopo di impostare un processo, analizzare i rischi e gestire, nel tempo, con continuità e nel fermo rispetto dei diritti di ogni individuo, i dati personali trattati.

Con tale Regolamento vengono definite le **MISURE DI SICUREZZA** idonee a garantire la privacy dopo un'attenta analisi dei rischi e a seguito di un'autovalutazione finalizzata all'adozione delle migliori strategie volte a presidiare i trattamenti di dati effettuati.

## 1.2 PRESENTAZIONE DEL DISCIPLINARE

### *1.2.1 Oggetto e finalità*

Il presente **Disciplinare** è redatto dal Titolare del Trattamento dei dati e si occupa di definire le azioni per la gestione/valutazione dei rischi e per l'adozione delle misure di sicurezza. Definisce, inoltre, gli adempimenti necessari, sia a rilevanza interna che esterna, e individua le procedure per la tutela della riservatezza dei dati personali. Vengono definiti i criteri e le modalità operative adottate e individuate le procedure per la tutela della riservatezza dei dati personali.

Vengono definiti i criteri e le modalità operative adottate dall'Azienda per lo sviluppo del documento programmatico sulla sicurezza. In particolare vengono individuati, descritti e valutati i rischi e le conseguenti misure di sicurezza adeguate alla protezione della sicurezza delle aree, dei dati e delle trasmissioni, al fine di ridurre al minimo i rischi stessi.

### *1.2.2 Ambito Applicazione*

L'ambito di applicazione riguarda *qualsiasi trattamento di dati personali* che venga effettuato nell'ambito delle attività dell'**AZIENDA** quale Titolare del Trattamento.

### *1.2.3 Revisione del Documento*

Il **Disciplinare** deve essere aggiornato o modificato tempestivamente dal Titolare del Trattamento qualora, nel corso delle attività svolte, dovessero presentarsi anomalie applicative delle misure di sicurezza adottate o dovessero presentarsi ulteriori nuovi rischi tali da dover intervenire con nuove misure di sicurezza.

## 1.3 RIFERIMENTI NORMATIVI

- D. Lgs. 196/2003 – Codice Privacy;
- Regolamento (UE) 2016/679 del Parlamento Europeo, sì come rettificato da: rettifica, GU L 314 del 22.11.2016, pag. 72 (2016/679); rettifica, GU L 127 del 23.5.2018, pag. 3 (2016/679); rettifica, GU L 74 del 4.3.2021, pag. 35 (2016/679);
- D. Lgs. 101/2018 – decreto di armonizzazione del Codice Privacy al GDPR.

## 1.4 TERMINI E DEFINIZIONI

Si ritiene utile riportare, per favorire una migliore comprensione del disciplinare, le principali definizioni di ordine generale previste dal Regolamento.

1. **«dato personale»:** qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
2. **«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;
3. **«limitazione di trattamento»:** il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
4. **«profilazione»:** qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
5. **«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;
6. **«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;
7. **«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;
8. **«responsabile esterno 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;
9. **«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;
10. **«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 esterno del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare del trattamento o del responsabile esterno del trattamento;
11. **«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;
12. **«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;

13. **«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;
14. **«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;
15. **«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;
16. «**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 esterno 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 esterno del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile esterno del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile esterno del trattamento nella misura in cui tale responsabile esterno del trattamento è soggetto a obblighi specifici ai sensi del presente regolamento;
17. **«rappresentante»:** la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile esterno del trattamento per iscritto ai sensi dell'artico - lo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;
18. **«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;
19. **«gruppo imprenditoriale»:** un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;
20. **«norme vincolanti d'impresa»:** le procedure in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile esterno 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 esterno 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;
21. **«autorità di controllo»:** l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;
22. **«autorità di controllo interessata»:** un'autorità di controllo interessata dal trattamento di dati personali in quanto:
    a) il titolare del trattamento o il responsabile esterno 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;
    c) un reclamo è stato proposto a tale autorità di controllo;
23. «**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 esterno del trattamento nell'Unione ove il titolare del trattamento o il responsabile esterno del trattamento siano stabiliti in più di uno Stato membro;
    b) oppure trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile esterno del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

24. **«obiezione pertinente e motivata»:** un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile esterno del trattamento sia conforme al presente regolamento, 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;
25. **«servizio della società dell'informazione»:** il servizio definito all'articolo 1, paragrafo1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio (19);
26. **«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.

## 1.5 SIGLE E ABBREVIAZIONI

| | |
|---|---|
| **GDPR** | General data protection regulation |
| **PQ** | Procedura |
| **IO** | Istruzioni |
| **Privacy** | Trattamento dei dati personali svolto dall'azienda secondo il Regolamento (UE) 27/04/2016, n. 679, general data protection regulation (GDPR). |

## 1.6 AMBITO DI APPLICAZIONI E SCOPO

### *1.6.1 Ambito di Applicazione*

Il presente **Disciplinare** si applica ai dati personali, censiti e comunicati dagli Incaricati del Trattamento, nonché Responsabili, nelle modalità specificate dal *Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016* trattati da parte dell'azienda.

Tale documento è predisposto e tenuto aggiornato anche per definire, sulla base delle analisi dei rischi, della distribuzione dei compiti e delle responsabilità, nell'ambito delle strutture preposte al trattamento dei dati:

- criteri tecnici e organizzativi per la protezione dei dispositivi, delle aree e dei locali interessati dalle misure di sicurezza, nonché tutte le procedure per controllare l'accesso delle persone autorizzate agli stessi;
- i criteri e le procedure per assicurare l'integrità dei dati;
- i criteri e le procedure per la sicurezza delle trasmissioni dei dati;
- l'elaborazione di un piano di formazione verso tutti i referenti dell'organigramma della Privacy, al fine di renderli edotti dei rischi individuati e dei modi per prevenire danni.

### *1.6.2 Scopo*

Il presente Disciplinare è redatto con l'obiettivo di garantire la conformità agli obblighi di sicurezza e di protezione dei dati personali imposti dal Nuovo Regolamento Europeo sulla protezione dei dati.

L'approccio con il quale questo disciplinare è stato redatto si ispira al principio della *Privacy by design* che prevede di gestire la privacy a partire dalla progettazione di un processo aziendale.

Nell'ambito dei generali obblighi di sicurezza, il presente **Disciplinare** si propone di:

- assicurare l'adozione di misure di sicurezza tali da garantire un livello di protezione dei dati personali;
- rappresentare un valido strumento per l'adozione di idonee misure di sicurezza, in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, tali da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati

trattati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta dei dati medesimi;
- realizzare la protezione e la sicurezza dei dati attraverso misure di sicurezza di natura fisica, logica e organizzativa adottate dal Titolare del trattamento, dai Responsabili esterni del trattamento.

### *1.6.3 Le conseguenze della violazione della normativa*

Il GDPR ha previsto rilevanti sanzioni di natura amministrativa in caso di violazioni della normativa sulla protezione dei dati personali.

In particolare, l'art. 83 del GDPR distingue due gruppi di sanzioni amministrative:

- ✓ nel **primo gruppo** rientrano le violazioni cosiddette di minore gravità, per le quali sono previste le sanzioni amministrative pecuniarie di importi **fino a 10 milioni di euro o, per le imprese, fino al 2% del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore, e riguardano nello specifico le violazioni degli obblighi imposti ai seguenti soggetti:
  a) il titolare del trattamento ed il responsabile esterno del trattamento (artt. 8, 11, da 25 a 39, 42 e 43 GDPR);
  b) l'organismo di certificazione;
  c) l'organismo di controllo dei codici di condotta (art. 41 GDPR).
- ✓ nel **secondo gruppo** di sanzioni, più pesanti in considerazione della maggiore gravità delle fattispecie a cui sono ricondotte, le sanzioni ammontano **fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore, e riguardano nello specifico le seguenti violazioni:
  a) dei principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9;
  b) dei diritti degli interessati a norma degli articoli da 12 a 22;
  c) i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49;
  d) qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX;
  e) l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo (ovvero il Garante Privacy) ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1 GDPR.

Il **Garante per la protezione dei dati personali** è l'organo competente ad irrogare le sanzioni sopra citate, ai sensi dell'art. 15, co. 3 del d.lgs. 101/2018: lo stesso dovrà avere cura di valutare caso per caso le violazioni, affinché le sanzioni siano sempre effettive, proporzionate e dissuasive (art. 83, co. 1 GDPR), tenendo in debito conto le circostanze di cui all'art. 83, co. 2 GDPR, ossia la natura, la gravità, la durata della violazione, il carattere doloso o colposo della stessa, le categorie di dati personali interessate dalla violazione, ecc.

Dalla violazione della normativa in materia di protezione dei dati personali possono derivare anche **responsabilità penali.**

La materia penale è di stretta competenza nazionale e, pertanto, non viene disciplinata nel GDPR che si limita ad indicare che "*gli Stati membri stabiliscono le norme relative alle altre sanzioni per le violazioni del presente regolamento in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie…*"

Il **D. Lgs. 101/2018** modifica le fattispecie penalmente rilevanti già previste dal Codice Privacy, introduce nuove violazioni e abroga le fattispecie penali relative a obblighi non più sussistenti.

In base al nuovo impianto definito dal decreto di adeguamento, sono previsti i seguenti illeciti penali ai sensi del riformato Codice della Privacy:

- ✓ **Trattamento illecito di dati – Art. 167** (punito con la reclusione da sei mesi ad un anno e sei mesi);
- ✓ **Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala – Art. 167 bis** (punita con la reclusione da uno a sei anni);
- ✓ **Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala – Art. 167 ter** (punita con la reclusione da uno a quattro anni);
- ✓ **Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante – Art.168** (punita con la reclusione da sei mesi a tre anni;
- ✓ **Inosservanza dei provvedimenti del Garante – Art. 170** (punita con la reclusione da tre mesi a due anni);
- ✓ **Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori – Art. 171.**

La condanna per uno dei delitti previsti dal Codice Privacy importa la pubblicazione della sentenza.

## 1.7 PROCEDURA PER LA PROTEZIONE DEI DATI PERSONALI

### *1.7.1 SCOPO*

La procedura per la protezione dei dati personali specifica i requisiti generali di sicurezza e protezione dei dati personali adottati dall'azienda in adempimento a quanto richiesto nel nuovo regolamento.

Attraverso la **Procedura**, l'azienda definisce e applica i principali OBIETTIVI in tema di protezione dei dati:

L'**identificazione** degli aspetti connessi ai **rischi derivanti dal trattamento dei dati personali** già in fase di definizione/progettazione/revisione dei processi aziendali;
L'**adozione di misure di sicurezza idonee** a prevenire e ridurre al minimo i rischi inerenti al trattamento di dati personali;
L'adozione di opportuni criteri e modalità di ripristino dei dati in caso di danneggiamento e perdita accidentale;
**Sensibilizzazione** di dipendenti, fornitori, clienti in materia di protezione dei dati;
**Motivare e formare costantemente il personale dipendente** affinché venga sviluppato, ad ogni livello, il senso di responsabilità verso la tutela dei dati personali e la sicurezza delle informazioni;
Formazione ad un lecito e corretto trattamento dei dati personali e sicurezza delle informazioni;
evidenza della conformità legislativa attraverso un sistema di gestione per la protezione dei dati personali costantemente oggetto di analisi.

### *1.7.2 Applicabilità*

Il presente documento si applica a tutte le modalità di trattamento di dati personali da parte degli operatori dell'azienda e agli strumenti utilizzati e gli aspetti relativi alla sicurezza.

### *1.7.3 I principi della procedura di sicurezza e protezione dei dati*

I principi che sono alla base della procedura di sicurezza e protezione dei dati personali sono i seguenti, ossia i dati:

1. debbono essere trattati in modo lecito, corretto e trasparente nei confronti degli interessati;
2. debbono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in maniera tale da non essere 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, del Regolamento UE n. 2016/679, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
3. debbono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono stati trattati;
4. debbono essere esatti e aggiornati, oltre al fatto che vanno utilizzate misure per cancellare e rettificare dati inesatti;
5. debbono essere conservati in maniera tale che possano essere identificati dagli interessati per un arco temporale legato alla finalità del loro utilizzo. 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, del Regolamento UE n. 2016/679, 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»);
6. debbono essere 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»).

Il titolare del trattamento è competente per il rispetto dei principi enunciati ed è in grado di comprovarlo («responsabilizzazione»).

### *1.7.4 Concetto di "Liceità" del trattamento*

All'art. 6 del Regolamento si definisce il concetto di **"Liceità del Trattamento"**.
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 (per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale);*
*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.*

Se il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1, del Regolamento UE n. 2016/679, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro:

a) *di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;*
b) *del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento;*
c) *della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10 del Regolamento UE n. 2016/679;*
d) *delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;*
e) *dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.*

### 1.7.5 Condizioni per il consenso

Il **consenso** è una delle basi giuridiche del trattamento, nell'ambito del regolamento generale per la protezione dei dati personali.

### 1.7.6 Caratteristiche

Il consenso deve essere:

- ✓ inequivocabile;
- ✓ libero;
- ✓ specifico;
- ✓ informato;
- ✓ verificabile;
- ✓ revocabile.

- Consenso **inequivocabile**: vuol dire che non è necessario che sia esplicito ma può anche essere implicito (ma non tacito), purché, nel momento in cui sia desunto dalle circostanze, non sussista alcun dubbio che col proprio comportamento l'interessato abbia voluto comunicare il proprio consenso (es. l'inerzia non può costituire manifestazione di consenso. Deve prevedere una chiara azione positiva.
- Il consenso deve, invece, essere **esplicito** (art. 9 GDPR) nel caso di trattamento di dati sensibili o nel caso di processi decisionali automatizzati (es. profilazione).
- Il consenso deve essere dato **liberamente**, il che significa che l'interessato deve essere in grado di operare una scelta effettiva, senza subire intimidazioni o raggiri, né deve subire conseguenze negative a seguito del mancato conferimento del consenso.
  L'articolo 7 del GDPR chiarisce che "*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*".
- Il consenso deve essere **specifico**, cioè relativo alla finalità per la quale è eseguito quel trattamento. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per ogni finalità (Considerando 32 GDPR). Quindi, i dati dovranno essere pertinenti al consenso fornito, e in caso di modifiche del trattamento occorre richiedere un nuovo consenso.
- Il consenso deve essere **informato**, occorre cioè che l'interessato sia posto in condizioni di conoscere quali dati sono trattati, con che modalità e finalità e i diritti che gli sono attribuiti dalla legge. Inoltre l'interessato deve essere opportunamente informato sulle conseguenze del suo consenso. L'informazione si ha attraverso l'apposita informativa. Il regolamento europeo si concreta, più che sui requisiti formali del consenso, sulla necessità della validità sostanziale del consenso, per cui l'aspetto informativo è essenziale, richiedendo un linguaggio semplice e comprensibile, anche eventualmente colloquiale.
- Consenso **verificabile** non vuol dire che il consenso deve essere documentato per iscritto, né che è richiesta la forma scritta, ma che l'azienda deve essere in grado di dimostrare che l'interessato lo ha conferito con riferimento a quello specifico trattamento (quindi distinguendo tra i vari trattamenti). L'azienda dovrà essere in grado di sapere anche a quale informativa l'utente ha acconsentito, distinguendo tra le varie versioni.

- Il consenso deve essere **revocabile** in qualsiasi momento. La revoca deve essere facile così come lo è dare il consenso. Non vi è alcun obbligo di motivare la revoca, a seguito della quale il trattamento deve interrompersi (ovviamente la revoca non comporta illiceità del trattamento precedente, ma solo l'obbligo di terminare il trattamento), a meno che non sussista una differente base giuridica per continuare il trattamento. Per revocare il consenso, quindi, il titolare del trattamento dovrebbe predisporre una procedura analoga a quella offerta per concedere il consenso. In alternativa è possibile revocare il consenso inviando una comunicazione. Nel caso in cui il titolare del trattamento non ottemperi, ci si può rivolgere al Garante o al tribunale per la tutela dei propri diritti.

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 Regolamento UE n. 2016/679 è vincolante.

**Scadenza**
Occorre tenere presente che il consenso non dura per sempre. Quando si raccolgono dati personali occorre informare l'interessato della durata della conservazione (e quindi trattamento) del dato, scaduta la quale il dato va o anonimizzato oppure cancellato. Per questo motivo in alcuni casi potrebbe essere preferibile una base giuridica diversa dal consenso, come ad esempio i legittimi interessi del titolare del trattamento.

## 1.8 CONTESTO RELATIVO AL TRATTAMENTO DEI DATI PERSONALI

### *1.8.1 DATI TRATTATI*

I dati, che potrebbero essere trattati sia in maniera *elettronica* che *cartacea*, sono classificabili in:

**Dati Comuni** (informazioni non riguardanti una persona fisica identificata o identificabile).

**Dati Personali** (informazioni riguardanti una persona fisica identificata o identificabile).

**Dati Personali particolari** (informazioni idonee a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona).

### *1.8.2 Trattamento dei dati mediante l'utilizzo di nuove tecnologie*

Il **trattamento dei dati personali** mediante l'utilizzo di **nuove tecnologie** (es. *Videosorveglianza, Geolocalizzazione anche attraverso SIM aziendali*) presentano un **RISCHIO ELEVATO** per i diritti e le libertà dei soggetti.

Questa tipologia di trattamento dei dati non forma oggetto di legislazione specifica, ma al riguardo si applicano le disposizioni generali in tema di **protezione dei dati personali.** (*D.lgs 30 giugno 2003, n. 196 e smi*). Quindi con il **nuovo Regolamento Europeo** le attività da svolgere per essere a norma non cambiano ma diventano molto più precise e soggette a sanzioni.

Il **trattamento dei dati personali** mediante l'utilizzo di **nuove tecnologie** deve, in ogni caso, fondarsi **sui principi** di seguito esplicitati:

- ✓ **PRINCIPIO DI LICEITÀ**, in base al quale i dati devono essere trattati secondo le prescrizioni normative;
- ✓ **PRINCIPIO DI NECESSITÀ**, in base al quale i sistemi informativi e i programmi informatici devono essere configurati in modo tale da ridurre al minimo l'utilizzo dei dati personali;
- ✓ **PRINCIPIO DI PROPORZIONALITÀ**, in base al quale i dati personali oggetto di trattamento devono essere "*pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati*";
- ✓ **PRINCIPIO DI FINALITÀ**, in base al quale i dati devono essere raccolti e trattati per scopi determinati, espliciti e legittimi.

### *1.8.2.1 Videosorveglianza*

1.8.2.1.1 Definizione

Con il termine **"Videosorveglianza"** si definisce l'acquisizione, in modo continuativo, di immagini, eventualmente associate a suoni, relative a persone identificabili. Spesso il rilevamento comporta anche una contestuale registrazione ed una successiva conservazione dei dati. La raccolta, la registrazione, la conservazione e in generale, l'utilizzo di immagini configura un **"trattamento" di dati personali**, come specificato in più punti, è considerato "dato personale" qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione (art. 4, comma 1, lett. b) Codice Privacy).

Le **LINEE GUIDA 3/2019** sul trattamento dei dati personali attraverso "dispositivi video" adottate per la consultazione pubblica il 10/07/2019 evidenziano, innanzitutto, l'importanza del **principio di minimizzazione** dei dati, sottolineando che l'utilizzo dei dispositivi video deve limitarsi ai soli casi in cui ci siano esigenze prevalenti ad opera del titolare del trattamento rispetto ai diritti e le libertà degli interessati, e non vi siano soluzioni alternative che consentano ed implicano un impatto minore sulla privacy di questi ultimi (ad esempio, mediante l'impiego di personale addetto alla sicurezza).

1.8.2.1.2 Obbligo di informativa

Le nuove **LINEE GUIDA 3/2019** sul trattamento dei dati personali, **prescrivono di fornire e distribuire un'informativa su due livelli**. È da tempo che la legislazione europea sulla protezione dei dati indica che gli interessati devono essere a conoscenza del fatto che la videosorveglianza è in funzione, e devono essere informati in modo dettagliato in merito ai luoghi monitorati, e nell'art.12 del GDPR sono stabiliti ed indicati obblighi generali di trasparenza e informazione.

In dettaglio, un primo avviso, **definito di primo livello** (segnale di avvertimento) può contenere:

a. un'**icona grafica** esplicativa, ossia un'icona che sia facilmente visibile, comprensibile e chiaramente leggibile, ed indichi una panoramica significativa del trattamento previsto (articolo 12 GDPR);
b. i **contatti e l'identità del titolare del trattamento** e, ove previsto, del DPO;
c. i dettagli sulle **finalità** e sull'eventuale legittimo interesse del titolare del trattamento;
d. i **diritti dell'interessato**, informazioni sui maggiori impatti del trattamento, richiamo e riferimento alla seconda informativa, in particolare come e dove reperirla (preferenza alle fonti digitali, *QRcode*, o un link web che indirizza ad una informativa online ecc.).

Il formato delle informazioni deve essere adattato alla posizione individuale, praticamente **deve essere posizionato ad una distanza adeguata e ragionevole dal sistema di video device** in modo tale che l'interessato possa facilmente riconoscere in anticipo le circostanze della sorveglianza, prima di entrare nell'area monitorata (approssimativamente all'altezza degli occhi).

Le informazioni di **secondo livello**, contenute in un documento informativo completo, che può essere rappresentato da un foglio, un cartello, un poster, un link web o lo stesso QRcode, deve contenere informazioni più complete e dettagliate, collocato in un luogo facilmente accessibile e disponibile per gli interessati, ossia in una posizione centrale (ad es. ufficio informazioni, sulle scrivanie, reception, bacheche, etc.). In ogni caso il titolare del trattamento, anche per il tramite di un incaricato, ove richiesto è tenuto a fornire anche oralmente un'informativa adeguata, contenente gli elementi individuati dall'art. 13 del Codice privacy.

1.8.2.1.3 Obbligo di verifica preliminare

Altro obbligo stabilito nel Provvedimento Generale del Garante riguarda la ***"verifica preliminare"***.

E' ancora previsto che i trattamenti di dati personali nell'ambito di una attività di videosorveglianza debbano essere effettuati rispettando le misure e gli accorgimenti prescritti dal Garante come esito di una **verifica preliminare attivata d'ufficio** o a seguito di un interpello del titolare del trattamento (*art. 17 del Codice privacy*), **quando vi sono rischi specifici per i diritti e le libertà fondamentali**, nonché per la dignità degli interessati, in relazione alla natura dei dati o alle modalità di trattamento o agli effetti che può determinare.

Il Garante ha individuato i casi in cui si sono maggiori rischi:

quando i sistemi di raccolta delle immagini siano associati a dati biometrici;
quando i sistemi siano dotati di software che permettono il riconoscimento della persona tramite collegamento, incrocio o confronto delle immagini rilevate (come, ad esempio, la morfologia del voto) con altri specifici dati personali (in particolari, dati biometrici), ovvero sulla base del confronto della stessa immagine con una campionatura di soggetti precostituita alla raccolta di dati;
quando si abbia a che fare con sistemi cosiddetti "intelligenti", i quali non si limitano a riprendere e registrare le immagini, ma sono in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli;
quando si prevedono tempi di conservazione dei dati maggiori di sette giorni derivante da speciali esigenze di ulteriore conservazione, a meno che non derivi da una specifica richiesta dell'autorità giudiziaria o di polizia giudiziaria in relazione a un'attività investigativa in corso;
quando i trattamenti effettuati tramite videosorveglianza hanno natura e caratteristiche tali per cui le misure e gli accorgimenti individuati nel presente provvedimento non sono integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che possono determinare, il titolare del trattamento è tenuto a richiedere la verifica preliminare al Garante.

1.8.2.1.4 Tempi di conservazione

Particolare attenzione viene riservata anche ai limiti di **conservazione dei dati raccolti** tramite telecamere e videosorveglianza, che può superare le 72 ore solo in casi particolari (indagini di polizia e giudiziarie, sicurezza degli istituti di credito, ecc.).

1.8.2.1.5 NOMINE AD INCARICATO E A RESPONSABILE ESTERNO DEL TRATTAMENTO:
"*Il titolare del trattamento o il responsabile esterno del trattamento devono designare per iscritto tutte le Persone fisiche autorizzate sia ad accedere ai locali dove sono situate le postazioni di controllo, sia ad utilizzare gli impianti e, nei casi in cui sia indispensabile per gli scopi perseguiti, a visionare le immagini*" (art.30 del Codice sulla Privacy);

"*Vanno osservate le regole ordinarie anche per ciò che attiene all'eventuale designazione di responsabili del trattamento*" (art.29 del Codice sulla Privacy).

1.8.2.1.6 Obbligo DPIA
Il **Regolamento UE 2016/679**, in tema di videosorveglianza stabilisce che il **titolare del trattamento** è tenuto a procedere con un preventivo *Data Protection Impact Assessment* (**DPIA**) art. 35 Regolamento UE 2016/679 nelle ipotesi di sorveglianza sistematica su larga scala di zona accessibile al pubblico.

1.8.2.1.7 Notificazione al Garante
La notificazione al Garante per la videosorveglianza è necessaria per trattamenti peculiari, ossia la raccolta e l'utilizzo di dati che indichino la posizione geografica di persone ed oggetti mediante una rete di comunicazione elettronica (art. 37, comma 1, lett. a), D.lgs. 196/2003). A tal proposito, il Garante, con il parere del 23 aprile 2004, ha precisato che tale evenienza si traduce nella "*localizzazione di persone od oggetti, ed è quindi riferita alla rilevazione della loro presenza in determinati luoghi, mediante reti di comunicazione elettronica gestite o accessibili dal titolare del trattamento*" e che la stessa "*va notificata quando permette di individuare in maniera continuativa, anche con eventuali intervalli, l'ubicazione sul territorio o in determinate aree geografiche , in base ad apparecchiature o dispositivi elettronici detenuti dal titolare del trattamento, o dalla persona, oppure collocati sugli oggetti. La localizzazione deve comunque permettere di risalire all'identità degli interessati, anche indirettamente attraverso appositi codici.*"

In conseguenza di ciò, non devono essere notificati al Garante i trattamenti di dati personali che consentono solo una rilevazione non continuativa del passaggio o della presenza di persone o cose (come avviene con la registrazione degli ingressi e delle uscite presso i luoghi di lavoro).

### *1.8.2.2 Geolocalizzazione*
Anche il **fenomeno della geo-localizzazione** solleva questioni **in termini di privacy** e nel rispetto delle sempre più stringenti norme in tema di riservatezza, in quanto i dati delle coordinate geografiche, sebbene ad un primo esame possano sembrare anonimi, in realtà l'incrocio di questi con altri dati, ad esempio i dati del sistema turni, consentono di risalire all'identità di un dipendente a cui sia stato assegnato uno specifico dispositivo.

Molte aziende utilizzano il sistema di **geo-localizzazione GPS** dei propri veicoli.
Il **GPS** è uno strumento che permette di rilevare la posizione geografica del veicolo sul quale è installato e, grazie all'utilizzo di software dedicati, gestire la flotta aziendale.

A tal proposito il **Garante della privacy** ha affrontato tale questione e sottolineato gli adempimenti che le imprese debbono svolgere prima di installare i dispositivi e di iniziare il trattamento dei relativi dati.

In caso di installazione di dispositivi di localizzazione satellitare, le aziende devono:

effettuare la notificazione preliminare al Garante;

fornire ai lavoratori interessati dai trattamenti dei propri dati, un'**informativa** comprensiva di tutti gli elementi in ordine a tipologia di dati, finalità e modalità del trattamento, compresi i tempi di conservazione;
adottare le **misure di sicurezza** previste dal Codice al fine di preservare l'integrità dei dati trattati e prevenire l'accesso agli stessi da parte di soggetti non autorizzati.
Dovranno, inoltre, definire con precisione le modalità di raccolta, di elaborazione e di conservazione dei dati di geo-localizzazione e degli altri **dati personali**, differenziando le tutele in base alla singola finalità perseguita.

La questione forse più interessante trattata dal Garante con il provvedimento in questione riguarda appunto **tempi di conservazione** dei dati raccolti, il periodo di conservazione viene individuato a seconda della tipologia di dati trattati. Al termine del periodo individuato, i **dati personali** raccolti dovranno essere automaticamente cancellati o anonimizzati.

Dovranno essere adottate anche precise misure di sicurezza e l'accesso ai dati trattati dovrà essere consentito al solo personale incaricato, definendo per i dati di geo-localizzazione appositi profili autorizzativi individuali per ogni singolo utente.

#### *1.8.2.3 Telefoni Cellulari aziendali*

Il datore di lavoro ha il potere di controllare che l'attività lavorativa svolta dai dipendenti sia conforme alle direttive da lui impartite e può farlo anche mediante SIM aziendali inserite in telefoni cellulari dati in uso agli stessi.

L'**Autorità garante** propende per l'ammissibilità dei controlli sulle SIM aziendali alla duplice condizione che i dati non siano utilizzati per contestazioni disciplinari e siano conservati per un periodo massimo di sei mesi.

Viene affermato un principio di necessità del trattamento in base al quale le informazioni sul traffico telefonico possono essere analizzate **solo se necessarie, pertinenti e non eccedenti gli scopi dichiarati**. Tali requisiti ricorrono nel caso delle chiamate in uscita ma sono da escludersi per le chiamate in entrata senza specifici addebiti e in caso di tariffe flat.

In ogni caso, poiché il sistema è idoneo a realizzare un potenziale e indiretto controllo a distanza sull'attività dei dipendenti, dovrà comunque essere stipulato uno specifico **accordo sindacale** nel rispetto della disciplina di settore.

Resta fermo che l'azienda, prima dell'inizio dei descritti trattamenti, è tenuta in base alla normativa vigente a fornire ai propri dipendenti assegnatari di telefono aziendale **un'informativa contenente la policy di utilizzo** e a nominare il responsabile esterno del trattamento.

### *1.8.3 Descrizione sintetica del trattamento dei dati*

Al fine di garantire che il trattamento dei dati si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto di protezione dei dati, l'AZIENDA ha adottato apposite **PROCEDURE (Vedi Capitolo 2)**, volte a definire le modalità operative da adottare al fine di garantire un trattamento dei dati conforme al GDPR.

# 1.9 ORGANIZZAZIONE E PERSONALE - PRINCIPALI SOGGETTI DEL TRATTAMENTO DEI DATI

Nel presente capitolo si definiscono quelli che sono **i principali soggetti protagonisti del trattamento dei dati**, così come descritti nel Nuovo Regolamento e viene definito l'**ORGANIGRAMMA** dell'azienda rispetto all'applicazione della Normativa con l'individuazione delle varie figure:

- TITOLARE DEL TRATTAMENTO DEI DATI;
- RESPONSABILI ESTERNI DEL TRATTAMENTO DATI;
- AMMINISTRATORI DI SISTEMA;
- INCARICATI AL TRATTAMENTO DATI.

## *1.9.1 Organigramma Privacy dell'Azienda*

Si rimanda a quanto riportato nell'allegato **Organigramma Privacy.**

## *1.9.2 Titolare del trattamento dei dati*

### *1.9.2.1 Definizione*

Il **"Titolare del Trattamento dei Dati"** 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*".

Ciò che consente di individuare il soggetto titolare del trattamento è, pertanto, il **potere decisionale** a lui imputabile in ordine al trattamento dei dati personali.

### *1.9.2.2 Responsabilità e compiti*

L'**Articolo 24** del Regolamento stabilisce la **responsabilità generale del titolare del trattamento** per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto.

Il titolare del trattamento deve essere in grado di:

1. Dimostrare la **conformità delle attività di trattamento** con il Regolamento stesso e deve mettere in atto misure adeguate ed efficaci volte a garantire ciò. 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.
2. 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. Questi ultimi, aventi probabilità e gravità diverse, possono derivare da trattamenti di **dati personali suscettibili di cagionare un danno fisico, materiale o immateriale**.
3. **Determinare,** la probabilità e la gravità del rischio per i diritti e le libertà dell'interessato, sulla base di **una valutazione oggettiva**, con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento.
4. Dimostrare il rispetto degli obblighi attraverso l'adesione a Codici di Condotta o a un meccanismo di certificazione.
5. Adottare **procedure interne** e attuare misure che soddisfino i principi della protezione dei dati di default e fin dalla progettazione. Tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, creare e migliorare le caratteristiche di sicurezza, pseudonimizzare i

dati personali il più presto possibile, offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali e consentire all'interessato di controllare il trattamento dei dati.

6. Mettere in atto misure tecniche e organizzative adeguate al fine di 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.

### *1.9.3 Contitolari del trattamento*

#### *1.9.3.1 Definizione*

L'Articolo 26, poi, prevede l'ipotesi di **contitolari del trattamento**, che si configura *quando due o più titolari determinano congiuntamente le finalità e i mezzi del trattamento*: anche in questo caso è necessaria una **chiara ripartizione delle responsabilità**, che viene determinata sulla base di un accordo interno, con particolare riguardo all'esercizio dei diritti dell'interessato.

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

Indipendentemente dalle disposizioni del detto accordo, l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun titolare del trattamento.

### *1.9.4 Responsabile esterno del trattamento*

#### *1.9.4.1 Definizione*

Il **responsabile esterno del trattamento** è *la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento.*

#### *1.9.4.2 Responsabilità e compiti*

L'articolo 28 del Regolamento elenca i compiti del responsabile esterno del trattamento, enfatizzando la collaborazione che questi è tenuto a prestare al titolare del trattamento e prevedendo una sua peculiare *responsabilità diretta*. Egli deve possedere *"garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento"*.

Gli obblighi dei responsabili possono essere schematizzati secondo **3 grandi insiemi**:

- ✓ Obbligo di tracciabilità e trasparenza;
- ✓ Obbligo di garantire la sicurezza dei dati;
- ✓ Obbligo di avvisare, assistere e consigliare il titolare del trattamento.

❖ **TRACCIABILITA' E TRASPARENZA**

Il rapporto tra titolare del trattamento e responsabile esterno del trattamento è tracciabile e trasparente tramite la **contrattualizzazione dei reciproci obblighi.** Il contratto deve essere redatto in forma scritta, anche in formato elettronico.

In particolare, il responsabile esterno del trattamento deve:

ricevere per iscritto le istruzioni in ordine ai trattamenti che effettui per conto del titolare del trattamento, dato che dovrà poter dimostrare che tratta 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;
dovrà essere autorizzato per iscritto dal titolare del trattamento ad avvalersi di un sub-responsabile, nel caso in cui voglia designarne uno;
dovrà mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi che gli impone l'articolo 28 del Regolamento, e dovrà consentire e contribuire alle attività di revisione, comprese le ispezioni (o audit), realizzate dal titolare del trattamento;
dovrà anche tenere il registro dei trattamenti per conto del titolare del trattamento per cui tratta i dati.
rispettare le condizioni di cui ai paragrafi 2 e 4 dell'articolo 28 del Regolamento per ricorrere a un altro responsabile del trattamento;
mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo (in tale circostanza il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il detto Regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati);
consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento.
Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.
Fatto salvo un contratto individuale tra il titolare del trattamento ed il responsabile del trattamento, il contratto o altro atto giuridico in regolazione di detto rapporto può basarsi, in tutto od in parte, su clausole contrattuali stabilite dalla Commissione, secondo la procedura d'esame di cui all'art. 93, paragrafo 2, del Regolamento UE n. 2016/679, o su clausole contrattuali stabilite da un'autorità di controllo, in conformità del meccanismo di coerenza di cui all'art. 63 del citato Regolamento.
Fatta salva l'applicazione degli artt. 82 (Diritto al risarcimento e responsabilità), 83 (Condizioni generali per infliggere sanzioni amministrative pecuniarie) ed 84 (Sanzioni) della normativa in commento, se un responsabile del trattamento viola il citato Regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione.

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

- **GARANTIRE LA SICUREZZA DEI DATI**

Uno specifico obbligo del responsabile esterno del trattamento è quello riferito alla sicurezza dei dati: il responsabile esterno del trattamento non ha solo l'obbligo di adottare tutte le misure che consentano un livello di sicurezza dei dati personali che sia adeguata al rischio (art. 32 Regolamento UE n. 2016/679), ma deve anche garantire la riservatezza dei trattamenti (anche vincolando alla riservatezza i propri dipendenti), deve informare il titolare del trattamento di tutte le violazioni di dati di cui sia venuto a conoscenza, e, una volta terminata la prestazione di servizi, secondo le istruzioni ricevute dal titolare del trattamento, dovrà cancellare tutti dati o restituirli al titolare del trattamento, e cancellare tutte le copie esistenti (a meno che non sussista un obbligo di conservazione dettato dalla legge).

- **AVVISARE, ASSISTERE E CONSIGLIARE IL TITOLARE DEL TRATTAMENTO**

Al responsabile esterno del trattamento sono posti in capo anche obblighi che implicano una collaborazione col titolare del trattamento che si concreta nell'avvisare, assistere e consigliare il titolare del trattamento in merito al trattamento; ad esempio, in ordine al fatto di dover dare avviso al titolare del trattamento, se il responsabile esterno del trattamento ritiene che un'istruzione ricevuta dal titolare del trattamento violi una qualche norma sulla protezione dei dati, ne informa immediatamente il titolare del trattamento.

Egli, inoltre deve prestare assistenza al titolare del trattamento per consentirgli di evadere le richieste inerenti all'esercizio dei diritti degli interessati (*"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"*).

Tenendo conto della natura del trattamento e delle informazioni a sua disposizione, dovrà aiutare il titolare del trattamento a garantire la conformità con i requisiti di sicurezza del trattamento, notificare le eventuali violazioni di dati ed effettuare le valutazioni di impatto sulla protezione dei dati (**Vedi Capitolo 3 paragrafo1**).

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

## *1.9.5 Responsabile della protezione dei dati (Data Protection Officer)*

### *1.9.5.1 Definizione*

Il **Data Protection Officer** (**DPO**) è una figura autonoma e indipendente, che svolge i suoi compiti in assenza di conflitto di interesse. In tal senso non può ricoprire tale incarico un soggetto che si trova ai vertici aziendali, quindi in grado di influenzare le scelte adottate in materia di trattamento dei dati.

Il DPO è designato (art. 37) dal *titolare del trattamento* o dal *responsabile esterno del trattamento*, in base ad un contratto. La designazione dovrà essere comunicata all'Autorità di controllo nazionale.

Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:

a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10 del Regolamento UE N. 2016/679;

Un gruppo imprenditoriale può nominare un unico responsabile della protezione dei dati, a condizione che un responsabile della protezione dei dati sia facilmente raggiungibile da ciascuno stabilimento.

Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.

Nei casi diversi da quelli succitati, il titolare del trattamento, il responsabile del trattamento o le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o di responsabili del trattamento possono o, se previsto dal diritto dell'Unione o degli Stati membri, devono designare un responsabile della protezione dei dati. Il responsabile della protezione dei dati può agire per dette associazioni e altri organismi rappresentanti i titolari del trattamento o i responsabili del trattamento.

Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39 del detto Regolamento.

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

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

Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti.

Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.

Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.

#### *1.9.5.2 Responsabilità e Compiti*

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

Il **Data Protection Officer**, inoltre, ha il compito di:

- ✓ informare e consigliare il titolare dell'azienda o il responsabile esterno del trattamento, nonché i dipendenti, sugli obblighi previsti dalle norme in materia e quindi verificarne l'attuazione e l'applicazione. Quindi raccoglie informazioni sui trattamenti svolti e ne verifica la conformità alle norme;
- ✓ sorvegliare l'osservanza del citato 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 pareri ed assistere il titolare del trattamento in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliare i relativi adempimenti;
- ✓ cooperare con l'autorità di controllo;
- ✓ essere il punto di contatto, non solo per il Garante ma anche per gli interessati al trattamento, in merito a qualunque problematica connessa ai loro dati o all'esercizio dei loro diritti;
- ✓ consultare il Garante anche di propria iniziativa.

Occorre tenere presente che è una prassi consolidata che il DPO abbia il compito di realizzare l'inventario dei trattamenti e tenere il registro degli stessi.

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.

Il **DPO** non è, però, personalmente responsabile dell'inosservanza degli obblighi in materia di protezione dei dati personali, infatti è compito del titolare del trattamento (art. 24) mettere in atto le misure tecniche ed organizzative adeguate.

**Il DPO risponde solo per lo svolgimento dei suoi obblighi di consulenza ed assistenza nei confronti del titolare del trattamento**, che è (eventualmente in solido col responsabile esterno del trattamento) l'unico soggetto responsabile del rispetto della normativa. Il titolare del trattamento, quindi, potrà solo avanzare pretese risarcitorie basate sulla responsabilità contrattuale, nei confronti del DPO.

**L'AZIENDA non è tenuta alla nomina del DPO non trattando dati su larga scala.**

### *1.9.6 Amministratori di sistema*

#### *1.9.6.1 Definizioni*

Gli **Amministratori di Sistema** sono quei soggetti preposti alla sicurezza, alla gestione e alla manutenzione delle banche dati, dei sistemi e delle infrastrutture informatiche di un'impresa, di un ente o organismo cui vengono associati anche gli amministratori di reti e gli amministratori di sistemi software complessi (figura già definita dall'art. 1, comma 1, lett. c) d.P.R. 318/1999 nella disciplina previgente al Codice Privacy) che, in ragione delle proprie mansioni, come ad esempio, attività tecniche quali il salvataggio dei dati (backup/recovery), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e manutenzione *hardware*, possono avere il privilegio di accedere – accesso da considerarsi anche solo in via potenziale – ai dati personali trattati dal titolare del trattamento.

**Nel nuovo Regolamento europeo sulla protezione dei dati personali (GDPR) non sembra ci sia un chiaro riferimento alla figura dell'amministratore di sistema nel processo di trattazione e custodia dei dati, pur trattandosi di una figura implicitamente richiamata, in alcune norme, per le sue specifiche**

**competenze tecniche**, laddove al titolare del trattamento e/o all'eventuale responsabile esterno del trattamento nominato, spetta il compito di mettere in atto misure tecniche per **garantire un livello di sicurezza adeguato al rischio** (art. 32 del Regolamento). In questo ambito non si parla di quali siano le "misure adeguate" ma sicuramente sono superiori a quelle misure minime di sicurezza a cui si faceva riferimento nell'allegato B del codice del 2003 e cioè credenziali di autorizzazione, aggiornamenti software e via discorrendo.

L'**art. 32** del Regolamento descrive delle procedure altamente tecniche – quali la cifratura dei dati personali, il loro tempestivo ripristino in caso di incidenti fisici o tecnici e le verifiche periodiche delle misure tecniche ed organizzative adottate – che sicuramente lasciano intravvedere una necessaria partecipazione di personale specialistico esperto nella gestione e nella trattazione informatica dei dati personali, così come la necessità di un suo intervento tecnico sin dalle fasi di progettazione e protezione dei dati – la cosiddetta **privacy by design** e **privacy by default** – di cui all'art. 25 del medesimo Regolamento UE.

#### *1.9.6.2 Le funzioni dell'amministratore di sistema*

**L'Amministratore di Sistema riveste sul piano operativo una certa professionalità ed un ruolo rilevante all'interno dell'azienda**:

- ✓ rappresenta una figura essenziale per la sicurezza delle banche dati e la corretta gestione delle reti telematiche;
- ✓ è un esperto chiamato a svolgere delicate funzioni che comportano la concreta capacità di accedere a tutti i dati che transitano sulle reti aziendali;
- ✓ a lui viene affidato spesso anche il compito di vigilare sul corretto utilizzo dei sistemi informatici di un'azienda.

È evidente che si tratti di ***personale tecnico qualificato*** a sé stante che non potrà neanche coincidere con analoghe figure di controllo.

Oltre ad essere la prima persona che dovrebbe rendersi conto di un eventuale violazione o perdita dei dati, accidentale od intenzionale che sia, è proprio l'amministratore di sistema che, con la sua attività quotidiana, svolge routine di sicurezza informatica volte a garanzia della struttura informatica, cosiddetto "*data breach*" (**Vedi Capitolo 3, Paragrafo 3**).

### *1.9.7 Incaricati al trattamento dei dati*

#### *1.9.7.1 Definizione*

Gli **INCARICATI AL TRATTAMENTO DEI DATI sono persone autorizzate** al trattamento dei dati sotto l'autorità diretta del titolare del trattamento o del responsabile esterno del trattamento (art. 4. n. 10 GDPR).

Incaricato, o autorizzato, è il soggetto persona fisica che effettua materialmente le operazioni di trattamento sui dati personali.

L'incaricato può operare alle dipendenze del titolare del trattamento, ma anche del responsabile esterno del trattamento, se nominato. Ovviamente gli autorizzati possono essere organizzati con diversi livelli di delega.

Il ***regolamento europeo*** non prevede l'obbligo di nomina o designazione espressa, ma è fondamentale **fornire agli autorizzati le istruzioni operative** (art. 29 GDPR), compreso gli obblighi inerenti le misure di sicurezza, e che sia fornita loro la **necessaria formazione**. In caso contrario, infatti, anche in presenza di formali designazioni, queste sarebbero del tutto prive di valore.

La designazione degli incaricati può avvenire anche con unico atto per più persone. L'eventuale designazione non necessita di firma per accettazione, anche se è utile una **firma per presa visione**, quale prova della conoscenza dell'incarico e delle istruzioni fornite.

L'incaricato deve, ovviamente, attenersi strettamente alle istruzioni ricevute (**Vedi Capitolo 3, Paragrafo 2**).

## 1.10 FORMAZIONE DELLE FIGURE IMPEGNATE NEL GDPR

Il **Regolamento europeo** 679/16 (GDPR) prevede **l'obbligo della formazione** per le imprese in materia di protezione dei dati personali per tutte le figure presenti nell'organizzazione (sia dipendenti che collaboratori).

La **FORMAZIONE** viene considerata **un pre-requisito per potere operare all'interno delle organizzazioni, imprese**.

### *1.10.1 Base normativa*

Si tratta di una novità rilevante in quanto il decreto legge 9 febbraio 2012, n. 5, convertito, con modificazioni, dalla legge 4 aprile 2012, n. 35. aveva abrogato nel 2012 l'obbligo di formazione previsto al punto 19.6 del Disciplinare tecnico in materia di misure minime (allegato B al D.Lgs, 196 del 2004 "Codice della privacy) che prevedeva: "*interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività,* delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare del trattamento".

L'**art. 29** del Regolamento prevede, infatti, che "il responsabile esterno del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso ai dati personali **non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento …**".

Il Gruppo di lavoro ex 29 nel parere n. 3/2010 aveva individuato tra le misure comuni concernenti la responsabilità "*un'adeguata formazione ed istruzione del personale in materia di protezione dei dati. Il personale in questione dovrebbe includere gli incaricati (o responsabili) del trattamento dei dati personali, ma anche dirigenti e sviluppatori in campo informatico e direttori di unità commerciali*".

La centralità della formazione è confermata anche dall'**art. 32 "Sicurezza del trattamento"** paragrafo 4 che prevede che "*il titolare del trattamento ed il responsabile esterno del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se* ***non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri***".

### *1.10.2 Scopo*

La formazione è **finalizzata ad illustrare i rischi generali e specifici dei trattamenti di dati, le misure organizzative, tecniche ed informatiche adottate, nonché le responsabilità e le sanzioni**.

### *1.10.3 Obbligo formativo – Misure di sicurezza*

**L'obbligo formativo** non può essere sottovalutato dalle imprese, in quanto in caso di mancata erogazione della formazione **scatta, infatti, ai sensi dell'art. 83 par 4 del Regolamento europeo, la rilevante sanzione** amministrativa pecuniaria **fino a 10 milioni di euro o, per le imprese, fino a 2 % del fatturato mondiale annuo dell'anno precedente se superiore.**

L'adempimento degli obblighi formativi è sovente oggetto anche di accertamenti ispettivi da parte dell'Autorità Garante privacy e da parte della Guardia di Finanza che ha rinnovato nel 2016 il protocollo di intesa con l'Autorità.

La **formazione** costituisce, pertanto, una **misura di sicurezza per le organizzazioni**, un onere a carico del titolare del trattamento, un diritto e dovere per i dipendenti e i collaboratori.

A tal proposito l'AZIENDA effettua la formazione interna, finalizzata alla conoscenza dei requisiti fondamentali per il trattamento dei dati previsti nell'ambito del proprio settore di attività. Le attività da svolgere per gestire, formare e addestrare il proprio personale vengono definite nella Procedura **Gestione Formazione del Personale** alla quale si rimanda (Vedi Capitolo 2 Paragrafo 2 - PQ02).

# 1.11 PIANIFICAZIONE

## *1.11.1 Registro delle attività di trattamento*

I **registri delle attività di trattamento** si configurano come uno **strumento** che sono parte integrante di quel generale sistema di corretta gestione dei dati personali che le aziende o le organizzazioni dovranno creare. In concreto si tratta di registri che racchiudono tutte le informazioni relative ai trattamenti dei dati svolti dai titolari o, per loro conto, dai responsabili del trattamento. L'obbligo di tenuta dei registri, in forma scritta o anche in formato elettronico, sussiste infatti non solo per il **titolare del trattamento** ma anche per il **responsabile esterno del trattamento**.

Di fatto cioè, coloro che svolgono attività di trattamento per conto di altro soggetto dovranno tenere sia un registro relativo ai trattamenti di cui sono titolari, sia un registro relativo ai trattamenti che svolgono per conto di chi ha delegato determinate attività.

La tenuta dei registri, come indicato dal Garante, pur non costituendo un adempimento formale, è parte integrante di un sistema di corretta gestione dei dati personali pertanto, i titolari e i responsabili, a prescindere dalle dimensioni dell'organizzazione e dalla tipologia dei trattamenti, dovrebbero comunque dotarsi dei registri. Un'adeguata predisposizione degli stessi potrà essere, infatti, un elemento importante al fine di realizzare un corretto trattamento dei dati personali, in linea quindi con l'obiettivo di **responsabilizzazione** (la c.d. *accountability*), che è uno dei principi fondamentali del Regolamento 2016/679.

L'**art. 30** del **Regolamento Europeo 2016/679** disciplina questo importante strumento di *compliance aziendale* in materia di dati personali, prevedendo l'indicazione delle seguenti informazioni:

Il nome e i dati di contatto del titolare del trattamento e, se presente, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
Le finalità del trattamento;
La descrizione delle categorie di interessati e delle categorie di dati personali;
Le categorie di destinatari a cui i dati personali siano stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
Se presenti, i trasferimenti di dati personali verso paesi terzi e la loro identificazione e la documentazione delle garanzie adeguate;
I **termini ultimi** previsti per la cancellazione delle diverse categorie di dati;
Una descrizione generale delle misure di sicurezza tecniche e organizzative;

Modalità di Trattamento;

Strumenti Utilizzati.

Come già detto, l'obbligo di tenere i registri compete anche ai **responsabili del trattamento**; in quest'ultimo caso il contenuto è più limitato. In base a quanto disposto dall'art. **30 comma 2 del GDPR**, nel registro delle attività di trattamento svolte per conto del titolare del trattamento, devono essere riportati:

- Il **nome e i dati di contatto** del responsabile esterno del trattamento o dei responsabili esterni del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile esterno del trattamento, del rappresentante del titolare del trattamento e, ove applicabile, del Responsabile della Protezione 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;
- Una **descrizione generale delle misure di sicurezza** tecniche e organizzative di cui all'art. 32 par. 1.

Questo registro rappresenta dunque una delle novità e, al tempo stesso, uno degli adempimenti più importanti concernenti le attività di trattamento e deve essere tenuto 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.

L'AZIENDA ha predisposto un registro delle attività di trattamento per il Titolare del trattamento, (**Vedi allegato Registro Titolare Trattamento GDPR**); tanto, poiché, sebbene l'AZIENDA abbia meno di meno di 250 dipendenti, il trattamento che essa effettua include il trattamento di categorie particolari di dati personali relativi a condanne penali e a reati di cui all'articolo 10 del Regolamento UE n. 2016/679.

Si rimanda all'allegato Registri delle attività di trattamento.

### *1.11.2 Analisi dei rischi e misure di sicurezza aziendale*

Con il termine "**sicurezza**" si fa riferimento all'adozione da parte del titolare del trattamento di **"adeguate misure tecniche e organizzative"** funzionali a prevenire e arginare i rischi del trattamento stesso, come "*la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale*" (*considerando 83*).

Quindi, in applicazione del Regolamento UE n. 2016/679, 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.

La sicurezza dei dati ruota attorno *a tre concetti fondamentali*:

1. garantire la sicurezza dei dati, ovvero la loro **disponibilità**;
2. **integrità** dei dati;
3. **riservatezza** dei dati.

### *1.11.3 Misure di sicurezza*

Il **Regolamento** pone l'accento sulla responsabilizzazione (**accountability**) del *titolare del trattamento* e dei *responsabili del trattamento*, che si deve concretizzare nell'adozione di **comportamenti proattivi a dimostrazione della concreta** (e non meramente formale) adozione del regolamento.
In particolare si evidenzia la necessità di *attuare misure di tutela e garanzia dei dati trattati*, con un approccio del tutto nuovo che demanda ai titolari il compito di decidere autonomamente le modalità e i limiti del trattamento dei dati alla luce dei criteri specifici indicati nel Regolamento:

- *principio* ***"privacy by design"***, in base al quale i servizi dovranno essere progettati fin dall'inizio in modo da tutelare la privacy degli utenti, cioè il trattamento deve essere previsto e configurato fin dall'inizio prevedendo le garanzie per tutelare i diritti degli interessati;
- ***rischio del trattamento***, inteso come valutazione dell'impatto negativo sulle libertà e i diritti degli interessati.

Il GDPR ha un approccio basato sulla *valutazione del rischio* (**risk based**), con il quale si determina la misura di responsabilità del titolare del trattamento o del responsabile esterno del trattamento, tenendo conto della natura, della portata, del contesto e delle finalità del trattamento, nonché della probabilità e della gravità dei rischi per i diritti e le libertà degli utenti.

#### *1.11.3.1 Misure tecniche e organizzative*

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

Il *Titolare del trattamento* e il *Responsabile esterno del tratta*mento mettono in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, che comprendono (*art. 32*):

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

#### *1.11.3.2 Codice di condotta*

Nel **regolamento europeo n. 679/2016 all'art. 40** incoraggia l'elaborazione di **codici di condotta** destinati a contribuire alla corretta applicazione del Regolamento, in funzione delle specificità settoriali e delle esigenze specifiche delle imprese.

Le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento possono, quindi, elaborare i codici di condotta, modificarli o prorogarli, allo scopo di precisare l'applicazione delle disposizioni del Regolamento, ad esempio:

a) il trattamento corretto e trasparente dei dati;
b) i legittimi interessi perseguiti dal responsabile esterno del trattamento in contesti specifici;
c) la raccolta dei dati personali;
d) la pseudonimizzazione dei dati personali;
e) l'informazione fornita al pubblico e agli interessati;
f) l'esercizio dei diritti degli interessati;

g) l'informazione fornita e la protezione del minore e le modalità con cui è ottenuto il consenso dei titolari della responsabilità genitoriale sul minore;
h) le misure e le procedure di cui agli **articoli 24** e **25** del GDPR e le misure volte a garantire la sicurezza del trattamento di cui all'**articolo 32**;
i) la notifica di una violazione dei dati personali alle autorità di controllo e la comunicazione di tali violazioni dei dati personali all'interessato;
j) il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali;
k) le procedure stragiudiziali e di altro tipo per comporre le controversie tra titolari del trattamento e interessati in materia di trattamento, fatti salvi i diritti degli interessati ai sensi degli **articoli 77** e **79** del GDPR.

Il codice di condotta contiene i meccanismi che consentono all'organismo di cui all'articolo 41, paragrafo 1, del Regolamento UE di effettuare il controllo obbligatorio del rispetto delle norme del codice da parte dei titolari del trattamento o dei responsabili del trattamento che si impegnano ad applicarlo, fatti salvi i compiti e i poteri delle autorità di controllo competenti ai sensi degli articoli 55 o 56 del citato Regolamento.

Le associazioni e gli altri organismi previsti dal Regolamento che intendono elaborare un codice di condotta o modificare o prorogare un codice esistente sottopongono il progetto di codice all'autorità di controllo (cioè al nostro Garante). L'autorità di controllo esprime un parere sulla conformità al regolamento del progetto di codice, della modifica o della proroga e approva tale progetto, modifica o proroga, se ritiene che offra in misura sufficiente garanzie adeguate.

Oltre all'adesione ai codici di condotta e aventi validità generale da parte di titolari o responsabili soggetti al presente regolamento, possono aderire a tali codici di condotta anche i titolari del trattamento o i responsabili del trattamento che non sono soggetti al citato regolamento ai sensi dell'articolo 3, al fine di fornire adeguate garanzie nel quadro dei trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali alle condizioni di cui all'articolo 46, paragrafo 2, lettera e) del Regolamento UE n. 2016/679. Detti titolari del trattamento o responsabili del trattamento assumono l'impegno vincolante e azionabile, mediante strumenti contrattuali o di altro tipo giuridicamente vincolanti, di applicare le stesse adeguate garanzie anche per quanto riguarda i diritti degli interessati.

Rispetto al Codice di Condotta adottato dall'AZIENDA si rimanda al **Capitolo 4**.

## *1.11.4 Valutazione d'impatto*

### *1.11.4.1 Definizione*

La **valutazione d'impatto sulla protezione dei dati** (**DPIA**, acronimo di *"Data Protection Impact Assessment"*) è un processo che il titolare del trattamento deve effettuare quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare *un rischio elevato per i diritti e le libertà delle persone fisiche* (**art. 35** GDPR).

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

La valutazione deve contenere almeno:

a) una **descrizione sistematica dei trattamenti previsti** e delle **finalità del tra**ttamento, compreso, se del caso, l'interesse legittimo perseguito dal titolare del trattamento;
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati;

d) le **misure previste per affrontare i rischi**, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli Interessati e delle altre persone in questione.

Inoltre la **valutazione d'impatto sulla protezione dei dati** è richiesta in particolare nei seguenti casi:

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata sul trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono allo stesso modo significativamente su dette persone fisiche;
b) il trattamento, su larga scala, di categorie particolari di dati di cui all'**articolo 9**, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'**articolo 10**;
c) la sorveglianza sistematica di una zona accessibile al pubblico su larga scala.

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

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

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

### ❖ CONSULTAZIONE PREVENTIVA

Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 del citato Regolamento indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.
Se ritiene che il trattamento previsto di violi il citato regolamento, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, l'autorità di controllo fornisce, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto al titolare del trattamento e, ove applicabile, al responsabile del trattamento e può avvalersi dei poteri di cui all'articolo 58 del Regolamento GDPR.
Tale periodo può essere prorogato di sei settimane, tenendo conto della complessità del trattamento previsto. L'autorità di controllo informa il titolare del trattamento e, ove applicabile, il responsabile del trattamento di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione.
La decorrenza del termini può essere sospesa fino all'ottenimento da parte dell'autorità di controllo delle informazioni richieste ai fini della consultazione.

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

d) ove applicabile, le rispettive responsabilità del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo imprenditoriale;
e) le finalità e i mezzi del trattamento previsto;
f) le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del presente regolamento;
g) ove applicabile, i dati di contatto del responsabile della protezione dei dati;
h) la valutazione d'impatto sulla protezione dei dati di cui all'articolo 35 del detto Regolamento;

i) ogni altra informazione richiesta dall'autorità di controllo.

#### *1.11.4.2 Oggetto DPIA*

La **DPIA,** per quanto può riguardare una sola operazione di trattamento dei dati, potrebbe essere utilizzata per valutare molteplici operazioni di trattamento che sono simili in termini di rischi presentati, purché adeguatamente considerate la specifica natura, portata, contesto e finalità del trattamento.

Quando un trattamento è svolto in contitolarità, è necessario che ciascun contitolare del trattamento definisca con precisione gli obblighi rispettivamente incombenti.

La **DPIA** stabilisce chi ha la responsabilità delle singole misure finalizzate alla gestione dei rischi e alla tutela dei diritti e delle libertà degli interessati. Ciascun titolare del trattamento dovrebbe indicare con chiarezza le rispettive esigenze e condividere tutte le informazioni utili senza pregiudicare quanto coperto da segreto né rivelare eventuali vulnerabilità.

#### *1.11.4.3 Trattamenti soggetti a DPIA*

La **valutazione d'impatto** è necessaria quando i rischi sugli effetti dell'interessato al trattamento sono alti, oppure si ricade nell'ambito di applicazione obbligatoria di impatto.

La **DPIA** è obbligatoria quando un trattamento *"possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (art. 35, paragrafo 1),* come meglio chiarito dal paragrafo 3 dell'**art. 35** e integrato da quanto prevede il paragrafo 4 dello stesso articolo.

Nel caso specifico l'AZIENDA non è tenuta alla *"Valutazione d'impatto"* in quanto non ricorrono rischi elevati per gli interessati in relazione ai trattamenti effettuati e non si ricade nel campo di applicazione espresso dall'art. 35 del Regolamento.

L'Azienda, tuttavia, ha deciso di effettuare la valutazione d'impatto poiché tratta dati personali relativi a persone fisiche, nonché categorie particolari di dati personali di cui all'art. 9, paragrafo 1, e dati relativi a condanne penali. Si rimanda all'**allegato DPIA-GDPR**.

#### *1.11.4.4 Quando viene effettuata una DPIA e chi la deve condurre*

La **DPIA** dovrebbe essere condotta "prima di procedere al trattamento" (art. 35, paragrafo 1, e art. 35, paragrafo 10; considerando **80** e **93**). Tale impostazione è coerente con i principi della privacy ***by design*** e ***by default*** (**art. 25** e **considerando 78**).

L'aggiornamento della **DPIA** nel corso dell'intero ciclo di vita di un determinato progetto garantirà la dovuta considerazione delle tematiche di trattamento e protezione dei dati favorendo l'individuazione di soluzioni che promuovano l'osservanza.

Lo svolgimento della DPIA è un processo continuativo e non un'attività una tantum.

**Spetta al titolare del trattamento garantire l'effettuazione della DPIA** (art. 35, paragrafo 2). La conduzione materiale della DPIA può essere affidata a un altro soggetto, interno o esterno all'organismo; tuttavia, la responsabilità ultima dell'adempimento ricade sul titolare del trattamento.

Il titolare del trattamento deve consultarsi con il responsabile della protezione dei dati (RPD/DPO), ove designato (art. 35, paragrafo 2); tale consultazione e le conseguenti decisioni assunte dal titolare del trattamento devono essere documentate nell'ambito della DPIA. Il RPD è chiamato anche a monitorare lo svolgimento della DPIA (**art. 39, paragrafo 1, lettera c**).

# 1.12 VALUTAZIONI DELLE PRESTAZIONI

## *1.12.1 Monitoraggio, misurazione, analisi e valutazione*

### *1.12.1.1 Generalità*

L'AZIENDA pianifica e attua idonei processi di monitoraggio e misurazione dei processi del ***Sistema di Gestione del trattamento dei dati***.

I dati risultanti da queste attività sono oggetto di analisi al fine di dimostrare:

- la conformità alle procedure aziendali in tema di GDPR;
- il raggiungimento degli obiettivi;
- la pianificazione continua e il miglioramento dei sistemi.

La Direzione promuove il Sistema e si impegna a fornire all'organizzazione tutte le risorse necessarie alla sua attuazione e al continuo miglioramento della sua efficacia.

La Direzione fornisce evidenza del suo impegno:

- comunicando all'organizzazione l'importanza di ottemperare ai requisiti del cliente e a quelli cogenti applicabili;
- stabilendo le procedure per la privacy;
- assicurando che siano definiti gli obiettivi per la privacy;
- effettuando i riesami del Sistema;
- assicurando la disponibilità delle risorse necessarie.

### *1.12.1.2 Monitoraggi e Misurazioni – Audit interni*

L'AZIENDA attraverso Audit periodici tiene monitorato il *Sistema di Gestione del Trattamento dei Dati* al fine di assicurare che lo stesso sia sempre conforme alle normative vigenti e alle procedure aziendali, quindi per assicurarsi della sua continua idoneità, adeguatezza ed efficacia.

# 1.13 MIGLIORAMENTO

## *1.13.1 Generalità*

Il concetto di **"Miglioramento continuo"** è importante anche nel contesto del "Trattamento dei Dati". Viene definita l'attività ricorrente mirata ad accrescere la capacità di una Organizzazione di soddisfare i requisiti richiesti dal *Regolamento UE 679/2016*.

L'AZIENDA migliora con continuità l'efficacia del *Sistema di Gestione del Trattamento dei Dati*, utilizzando le procedure per la privacy, le registrazioni relative ai risultati delle verifiche ispettive interne. Quando si verifica una non conformità l'azienda è organizzata per reagire, valutare l'esigenza di azioni per eliminare la causa, attuare ogni azione necessaria, riesaminare l'efficacia di ogni azione correttiva intrapresa, aggiornare, se necessario, i rischi e le opportunità determinati nel corso della pianificazione, effettuare, se necessario, modifiche al sistema di gestione della privacy.

Sempre in un'ottica di miglioramento, la società prende in carico tutte le richieste degli interessati e le processa nel rispetto delle tempistiche previste dal *Regolamento (UE) 27/04/2016, n. 679*.

Tutte le comunicazioni in ingresso e in uscita relative a richieste degli interessati sono protocollate.

# 2 PROCEDURE

## 2.1 PQ-01 GESTIONE E PROTEZIONE DEI DATI

### 2.1.1 SCOPO

Scopo della presente procedura è quello di definire le modalità operative da adottare per garantire che il trattamento dei dati personali si svolga nel rispetto dei *diritti e delle libertà fondamentali, nonché della dignità dell'interessato*, con particolare riferimento alla **riservatezza,** all'**identità personale** ed al **diritto di protezione dei dati personali**, così come previsto dal *Regolamento UE N. 679/2016.*

Questa procedura è applicata per il trattamento di tutti i dati particolari effettuato dall' **AZIENDA**, con le eventuali precisazioni, limitazioni, esclusioni definite nella procedura stessa.

### 2.1.2 RIFERIMENTI

- ✓ REGOLAMENTO EUROPEO UE 679/2016
- ✓ Linee guida sui Responsabili della Protezione dei Dati (RPD) adottate dal Gruppo Articolo 29 del 13/12/2016

### 2.1.3 SHEMA GENERALE DI RIFERIMENTO

Lo schema generale di riferimento per la gestione degli adempimenti per il trattamento dei dati prevede l'esecuzione delle seguenti attività:

7. Identificare gli interessati dal trattamento e fornirgli un'adeguata informativa;
8. raccogliere i relativi consensi (ad esclusione dei casi in cui ciò non è richiesto);
9. definire l'organizzazione per il trattamento dei dati;
10. adozione delle misure di sicurezza previste;
11. adempimenti periodici;
12. monitoraggio e miglioramento del Sistema

### 2.1.4 INFORMATIVA E CONSENSO

Prima di ogni cosa è necessario identificare gli interessati dal trattamento dei dati personali.

Per **"interessati"** si intendono: *"le persone fisiche, le persone giuridiche, l'ente o l'associazione cui si riferiscono i dati personali".*

Pre-requisito fondamentale per poter legalmente detenere e trattare dati personali è che sia stata fornita un'adeguata informativa agli interessati.

L'**AZIENDA**, pertanto, ha proceduto a fornire un'informativa in materia di trattamento dei dati personali a tutti gli interessati, ovvero, principalmente:

DIPENDENTI/COLLABORATORI

CLIENTI

FORNITORI

Per comodità sono messi a disposizione dell'Azienda dei FAC-SIMILE in allegato **(INFORMATIVE)** da utilizzare ogniqualvolta viene instaurato un rapporto con le figure sopraindicate.

### *2.1.4.1 Informativa a dipendenti e personale interno*

Ai dipendenti e al personale interno viene fornita una informativa utilizzando il modello di informativa per dipendenti e collaboratori allegati alla presente procedura.

La distribuzione delle informative viene effettuata prima dell'avvio dei trattamenti dei dati o comunque al momento dell'assunzione/inserimento.

Ne viene rilasciata copia agli interessati. Le Informative raccolte sono archiviate a cura dei Responsabili Interni.

2.1.4.1.1 Selezione del personale

Relativamente al **processo di selezione e reclutamento**, il primo contatto tra azienda e candidato avviene con l'invio del *curriculum* e l'eventuale *colloquio di lavoro.*

A tal proposito con **il D.lgs 101/2018** è stata apportata una modifica al Codice Privacy, tanto che i CV inoltrati ad aziende e società non devono contenere alcuna dicitura relativa **all'autorizzazione al trattamento dei dati personali**, quindi il consenso risulta **implicito con l'invio del CV.**
Ne deriva pertanto che l'AZIENDA può legittimamente trattare e conservare i dati riportati nei CV anche qualora il curriculum ricevuto da un candidato sia privo di esplicita autorizzazione al trattamento dei dati. Mentre, l'AZIENDA fornisce ai candidati una adeguata informativa privacy e lo fa al primo contatto utile ossia quando il candidato è chiamato a sostenere il colloquio.

### *2.1.4.2 Informativa e consenso a clienti*

2.1.4.2.1 Informativa

Generalmente la raccolta dei dati di un *cliente/potenziale cliente* è finalizzata:

- ✓ alla gestione dei rapporti di natura commerciale (richieste di contatto, contratti, informazioni sui prodotti, sui servizi aziendali etc.);
- ✓ alla gestione dei rapporti economici-amministrativi (fatturazione, pagamenti, insoluti…);
- ✓ per la gestione dei rapporti di altra natura (marketing, customer satisfaction, etc…)

L'**Informativa ai Clienti** in merito al trattamento dei dati personali viene resa al momento del primo contatto con un Cliente ovvero un potenziale Cliente.

A seconda di quanto possibile/opportuno, l'Informativa viene resa:

predisponendo una informativa da consegnare materialmente al Cliente/potenziale Cliente al momento del primo contatto, ovvero al momento della raccolta dei dati personali;

inserendola nei modelli di preventivo/contratto;

rendendola disponibile nel sito web aziendale;

visionata al primo accesso in piattaforma con obbligo di consenso esplicito ed archiviazione in DB.

2.1.4.2.2 Consenso

Il consenso del Cliente al trattamento dei suoi dati viene richiesto direttamente alla sottoscrizione del Contratto, che riporta tutte le informazioni utili all'interessato:

*TITOLARE DEL TRATTAMENTO DEI DATI, RESPONSABILE ESTERNO DEL TRATTAMENTO, riferimenti telefonici ed altro.*

#### 2.1.4.3 *Fornitori*

Per i Fornitori valgono le stesse considerazioni espresse per i Clienti, sia per quanto riguarda l'informativa sia per quanto riguarda il consenso.

L'informativa sarà formulata utilizzando come riferimento il Modello di "*Informativa dei fornitori*", che verrà trasmesso tramite e-mail richiedendo la sottoscrizione del consenso al trattamento. Qualora il consenso non fosse espresso e rispedito al mittente sarà considerato come "non acquisito".

### 2.1.5 ORGANIZZAZIONE PER IL TRATTAMENTO DEI DATI

Dopo aver provveduto a fornire le informative necessarie e ad aver raccolto i relativi consensi, vengono realizzate le condizioni che consentono una gestione "sicura" dei dati raccolti, ovvero che consentono di ridurre al minimo i rischi di perdita, danneggiamento, furto, accessi e trattamenti non autorizzati.

Il **Titolare del trattamento**, pertanto, **ha provveduto a**:

definire e rendere operativa un'adeguata "organizzazione" per il trattamento dei dati;

definire e rendere operative le misure di sicurezza previste dalla Normativa applicabile;

monitorare e sorvegliare la gestione dei dati personali, definendo opportune azioni di miglioramento (organizzativo e tecnologico).

### 2.1.6 STESURA DELLA DPIA

Viene effettuata una valutazione d'impatto relativa al trattamento dei dati effettuato dall'AZIENDA, che ci permette di valutare la gravità dei rischi per i diritti e le libertà delle persone fisiche e la probabilità che questi ultimi si verifichino. Dopo aver ben chiaro quali sono i rischi e le conseguenze che ne derivano, l'AZIENDA sarà in grado di determinare le opportune misure di sicurezza da adottare per ridurre e talvolta annullare il rischio stesso.

### 2.1.7 ADOZIONE DELLE MISURE DI SICUREZZA NEI TRATTAMENTI CON STRUMENTI ELETTRONICI

L'adozione delle misure di sicurezza nel trattamento dei dati con strumenti elettronici prevede la realizzazione delle seguenti attività:

- ✓ Utilizzo di un sistema di autenticazione informatica
- ✓ Sistema di autorizzazione
- ✓ Installazione ed aggiornamento periodico di programmi antivirus e firewall;
- ✓ back up periodici dei dati
- ✓ misure per dati sensibili e giudiziari.

#### 2.1.7.1 *Autenticazione informatica*

Gli incaricati che trattano dati personali con strumenti elettronici devono accedere a tali dati utilizzando delle credenziali di autenticazione ovvero tramite l'utilizzo di Username e Password.

Lo Username identifica l'utente ed è generalmente di dominio pubblico.

La Password è strettamente riservata, è di almeno 8 caratteri e non deve essere facilmente riconducibile all'interessato.

Nelle Istruzioni Operative dell'Amministratore di Sistema vengono riportate anche quelle relative alla tutela e salvaguardia delle credenziali di autenticazione ed alcune semplici regole per la generazione di password.

Ad ogni incaricato possono essere assegnate una o più credenziali di autenticazione.

Le password vanno modificate **almeno ogni sei mesi**.

Qualora l'accesso al PC sia possibile solo tramite uso di password riservate, copia delle password deve essere comunicata anche al Titolare del trattamento, il quale ha il compito di redigere un elenco credenziali di autenticazione e di custodirle in un luogo riservato, protetto e sicuro.

Qualora fosse necessario accedere ai dati in assenza del diretto interessato, il Titolare del trattamento provvederà ad utilizzare la copia delle password in suo possesso, dandone comunicazione all'interessato.

#### *2.1.7.2 Sistema di Autorizzazione*

Se ritenuto necessario, devono essere previsti dei profili di autorizzazione che consentano l'accesso differenziato, per incaricato o per classi omogenee di incaricati, ai soli dati necessari per effettuare le operazioni di trattamento per le quali sono stati incaricati.

La configurazione, aggiornamento e gestione dei profili di autorizzazione è di competenza dell'Amministratore di Sistema.

Almeno annualmente deve essere verificata dal Titolare del trattamento la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

#### *2.1.7.3 Antivirus e Firewall*

2.1.7.3.1 Antivirus

Ogni postazione di lavoro deve essere dotata di adeguato antivirus.

Gli antivirus installati dovrebbero essere aggiornati almeno mensilmente.

A tale proposito sono state definite delle *"Linee guida per la prevenzione dei virus"* all'interno del "Raccolta Istruzioni per la sicurezza dei dati personali" cui si fa riferimento.

2.1.7.3.2 Firewall

Nel caso in cui sia presente una rete interna con accesso ad Internet, deve essere prevista la possibilità di installare un firewall di protezione.

La configurazione, aggiornamento e gestione del firewall, antivirus e dell'intera rete è di competenza dell'Amministratore di Sistema.

#### *2.1.7.4 Back-up periodico dei dati*

Il Titolare del trattamento, con il supporto eventuale del responsabile esterno del trattamento e degli Incaricati, definisce gli archivi informatici da sottoporre a back-up periodico e le modalità operative definendo eventualmente specifiche istruzioni scritte. La frequenza minima con cui effettuare i back-up è giornaliera.

#### *2.1.7.5 Misure per dati sensibili e giudiziari*

Eventuali **dati sensibili o giudiziari** trattati con strumenti elettronici devono essere protetti in modo adeguato.

I supporti fisici fissi o rimovibili su cui tali dati sono memorizzati devono essere protetti tramite password adeguate (*vedi IO-03 relativo all'amministratore di sistema*) e custoditi in modo da evitare accessi non autorizzati. Inoltre si prevede che tali supporti, se non utilizzati, siano distrutti o comunque resi inutilizzabili.

### *2.1.8 ADOZIONE DELLE MISURE DI SICUREZZA NEI TRATTAMENTI DEI DOCUMENTI CARTACEI*

L'adozione delle misure di sicurezza nel trattamento dei dati senza strumenti elettronici prevede la realizzazione delle seguenti attività:

Definizione di adeguate istruzioni scritte agli incaricati finalizzate al controllo ed alla custodia, dei documenti contenenti dati personali durante tutte le operazioni necessarie per i trattamenti da effettuare.

Nel caso in cui gli incaricati trattino documenti contenenti dati sensibili o giudiziari, è responsabilità specifica dell'Incaricato controllarli e custodirli in modo che non siano accessibili a persone prive di autorizzazione;

L'accesso ai dati sensibili o giudiziari deve essere controllato.

Le persone ammesse a qualunque titolo devono essere identificate e registrate.

#### *2.1.8.1 Trattamento documenti cartacei*

Il Regolamento Generale sulla Protezione dei Dati **si applica, oltre ai dati detenuti in forma elettronica** anche a quelli **cartacei**.

Gli archivi cartacei debbono essere conservati in modo sicuro e, quando non più necessari, distruggerli in sicurezza.

I **documenti cartacei** devono essere:

f) ***conservati*** *in archivi adeguatamente protetti, per evitare la lettura e/o il prelievo non autorizzato, garantendo, quindi, la riservatezza e l'integrità dei Dati Personali e/o "categorie particolari di dati personali", c.d. Dati Sensibili, e/o Dati Giudiziari, in essi contenuti;*

g) ***riposti*** *negli appositi archivi che dovranno essere chiusi a chiave, in armadi o stanze, al termine della giornata lavorativa. Le chiavi dovranno essere risposte in un luogo sicuro e non lasciate nelle serrature stesse.*

#### *2.1.8.2 Consultazione dei documenti cartacei*

La consultazione dei documenti contenenti Dati Personali e/o "categorie particolari di dati personali", c.d. Dati Sensibili, e/o Dati Giudiziari, deve avvenire esclusivamente da parte degli Autorizzati, solo quando operativamente necessario e quando possibile in loco.

#### *2.1.8.3 Distruzione dei documenti cartacei*

In relazione alle previsioni di cui all'art. 5, paragrafo e), e 89 del Regolamento (UE) 2016/679, che prevedono la conservazione dei dati personali per un tempo ben definito, i documenti che non devono essere conservati per legge, devono essere distrutti al termine della loro utilizzazione.

La **distruzione dei documenti** nei limiti consentiti dalla legge, deve essere effettuata quando è espressamente richiesto dall'interessato e/o quando comunicato dal Titolare del trattamento ovvero dal Responsabile esterno del trattamento, all'interno della propria area di competenza e deve essere formalizzata

ed autorizzata dal Titolare del trattamento o dal Responsabile esterno del trattamento secondo competenza, in relazione alla titolarità dei dati contenuti nel documento in esame.

I documenti dovranno essere distrutti, sotto la supervisione del Responsabile esterno del trattamento all'interno della propria area.

La distruzione legittima dei documenti cartacei contenenti dati personali deve essere effettuata, attraverso opportuni strumenti (distruggidocumenti) e comunque in modo da rendere impossibile la ricostruzione del documento.

#### *2.1.8.4 Misure sicurezza antincendio*

L'**AZIENDA** è attenta alle Disposizioni Normative del D.lgs 81/08, pertanto ha previsto tutte le misure di sicurezza relativamente al Rischio di Incendio della Sede in cui opera, formando gli addetti all'Antincendio e dotando la struttura di opportuni presidi antincendio, garantendo così la protezione degli archivi cartacei, dei dischi rigidi e dei Personal Computer.

## 2.2 PQ-02 GESTIONE FORMAZIONE

### *2.2.1 Scopo*

Scopo della presente procedura è definire le modalità operative e le responsabilità all'interno dell'AZIENDA per la pianificazione, l'attuazione e la registrazione dell'attività formativa e/o di aggiornamento del personale interno (dipendenti) e esterno (commerciali) *in materia di protezione dei dati personali per tutte le figure presenti.*

### *2.2.2 Campo di applicazione*

La procedura si applica alle **attività connesse alla formazione** di tutte le risorse umane dell'azienda che trattamento dati personali. L'obiettivo è quello di far comprendere i contenuti della normativa di riferimento e le modalità di applicazione della stessa, in modo da garantire efficienza nel trattamento dei dati.

Dunque è finalizzata ad illustrare i rischi generali e specifici dei trattamenti di dati, le misure organizzative, tecniche ed informatiche adottate, nonché le responsabilità e le sanzioni.

Attraverso la Formazione, dunque, l'Azienda favorisce processi di integrazione e armonizzazione, per contribuire a costruire una cultura aziendale che rispecchi gli adempimenti richiesti dal Regolamento UE n. 679/2016.

### *2.2.3 Riferimenti*

- ✓ REGOLAMENTO EUROPEO UE 679/2016
- ✓ Linee guida adottate da Gruppo Articolo 29
- ✓ Linee guida Garante della Privacy

### *2.2.4 Responsabilità*

Il *Titolare del Trattamento*, come stabilito dall'Art. 28 del Regolamento UE, nel momento in cui affida le attività a un **Responsabile esterno del Trattamento**, ricorre a responsabili che presentino garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del GDPR, soprattutto in tema di sicurezza del trattamento.

### 2.2.5 *Modalità operative*

La **formazione** costituisce una **misura di sicurezza** per le organizzazioni, un onere a carico del titolare del trattamento, un diritto e dovere per i dipendenti e i collaboratori.

**L'obbligo formativo** non deve essere in alcun modo sottovalutato da parte delle imprese: nel caso di mancata erogazione della formazione **scatta, infatti, ai sensi dell'art. 83 par 4 del Regolamento privacy europeo, la rilevante sanzione** amministrativa pecuniaria **fino a 10 milioni di euro o, per le imprese, fino a 2 % del fatturato mondiale annuo dell'anno precedente se superiore.**

L'adempimento degli obblighi formativi è sovente oggetto anche di accertamenti ispettivi da parte dell'Autorità Garante privacy e da parte della Guardia di Finanza che ha rinnovato nel 2016 il protocollo di intesa con l'Autorità.

#### *2.2.5.1 Generalità*

L'attività di formazione del personale interno è rivolta a:

- ✓ fornire la preparazione necessaria nello svolgimento dei compiti assegnati rispettando quanto previsto dal Regolamento;
- ✓ permettere un continuo aggiornamento;
- ✓ assicurare la corretta comprensione ed applicazione dei principi previsti dal *Sistema di Gestione del Trattamento dei dati*.

L'Organizzazione, pertanto, deve:

- ✓ pianificare quanto prima un percorso ed un piano di formazione;
- ✓ prevedere prove finali nel percorso formativo, e sessioni di aggiornamento alla luce delle modifiche normative, organizzative e tecniche;

#### *2.2.5.2 Determinazione delle necessità di addestramento*

Nella progettazione dei corsi di formazione, occorre esaminare ed individuare: i **fabbisogni formativi** che possono essere originati sia da programmi generali sia da specifiche necessità, sia da richieste/proposte da parte del personale, che le **modalità di erogazione**.

Vengono stabilite aree di priorità di intervento, a titolo esemplificativo ma non esaustivo, le figure apicali, gli amministratori di sistema, i nuovi assunti ed infine le persone autorizzate al trattamento dei dati personali.

La previsione di eventi formativi diretti al personale e ai collaboratori concretizza il principio di "accountability" ossia di responsabilizzazione del Titolare del trattamento, previsto dal Regolamento europeo n. 679/16.

Il programma ed il piano formativo costituiscono, pertanto, dei tasselli rilevanti del sistema di gestione del trattamento dei dati in grado di concretizzare il principio di accountability inteso come capacità di dimostrare di avere adottato misure di sicurezza adeguate.

#### *2.2.5.3 Formazione del personale*

La formazione del personale può avvenire anche mediante il ricorso a fornitori esterni di percorsi formativi, docenti singoli od enti di formazione. Inoltre la formazione del personale come anche quello di nuova

assunzione e quello assegnato a nuove mansioni, può venir eseguito mediante affiancamento a personale più esperto, con funzione di tutor.
In occasione di ogni corso di formazione tenuto presso la sede scelta dall'Azienda, viene redatto un Verbale di Formazione-informazione contenente i dati del Titolare del trattamento, dell'Incaricato Privacy, l'argomento trattato ed un elenco con firma di presenza dei dipendenti.

## 2.3 PQ-03 GESTIONE DATA BREACH

### *2.3.1 Scopo e campo di applicazione*

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

Il presente documento si prefigge lo scopo di indicare le opportune modalità di gestione del **data breach**, nel rispetto della normativa in materia di trattamento dei dati personali, garantendo in particolare l'aderenza ai principi e alle disposizioni contenute nel Regolamento UE 679/201

### *2.3.2 Normativa e documenti di riferimento*

- ✓ Regolamento UE 679/2016, considerando n. 85, 86, 87, 88 artt. 33, 34
- ✓ Guidelines on Personal data breach notification under Regulation 2016/679 –article 29 data protection working party (Adopted on 3 October 2017 –as last Revisedand Adopted on 6 February 2018)

### *2.3.3 Gestione del data Breach interno alla struttura*

#### *2.3.3.1 Modalità e profili di notifica all'autorità garante della privacy*

Ogni incaricato al trattamento qualora venga a conoscenza di un potenziale caso di data breach, avvisa tempestivamente il responsabile esterno del trattamento. Quest'ultimo, valutato l'evento, se confermate le valutazioni di potenziale data breach, lo segnala tempestivamente al Titolare del Trattamento.

La segnalazione perviene al Responsabile esterno del Trattamento tramite le consuete modalità di gestione dei flussi documentali già in uso in azienda.

Il Responsabile esterno del Trattamento effettua una valutazione dell'evento e sulla scorta delle determinazioni raggiunte predispone l'eventuale comunicazione all'Autorità, a firma del Titolare del trattamento, da inviare senza ingiustificato ritardo e, ove possibile, entro 72 ore, da determinarsi dal momento in cui il Titolare del trattamento ne è venuto a conoscenza, cioè quando abbia un ragionevole grado di certezza del verificarsi di un incidente di sicurezza che riguardi dati personali. Oltre il termine delle 72 ore, la notifica deve essere corredata delle ragioni del ritardo.

La notifica di cui al paragrafo 1 deve almeno:

j) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
k) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
l) descrivere le probabili conseguenze della violazione dei dati personali;

m) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

È comunque fatta salva la possibilità di fornire successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla violazione di cui il Titolare del trattamento venga a conoscenza, a seguito della effettuazione di ulteriori indagini e attività di follow-up (c.d. notifica in fasi).

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

La scelta e le motivazioni che hanno portato a non notificare l'evento deve essere documentata a cura del Responsabile esterno del Trattamento.

### *2.3.4 Gestione del data Breach esterno alla struttura*

Ogni qualvolta l'azienda/Titolare del trattamento si trovi ad affidare il trattamento di dati ad un soggetto terzo Responsabile esterno del Trattamento Esterno, è tenuta a stipulare con tale soggetto uno specifico contratto che lo vincoli al rispetto delle istruzioni impartitegli dal Titolare del trattamento in materia di protezione dati.

Ciò al fine di obbligare il Responsabile esterno del trattamento ad informare il Titolare del Trattamento senza ingiustificato ritardo, di ogni potenziale evento di data breach.

Ad ogni Responsabile esterno del Trattamento deve essere comunicato il contatto del Titolare dell'azienda al quale effettuare la predetta segnalazione (PEC a uopo designata dall'Azienda).

#### *2.3.4.1 Modalità e profili di notifica all'autorità garante della Privacy*

Ogni Responsabile esterno del Trattamento, qualora venga a conoscenza di un potenziale data breach che riguardi dati di cui l'azienda sia titolare del trattamento, ne dà avviso senza ingiustificato ritardo al Titolare dell'azienda.

Per "ingiustificato ritardo" si considera la notizia pervenuta al Titolare dell'azienda al più tardi entro 12 ore dalla presa di conoscenza iniziale da parte del responsabile esterno del trattamento.

Il Titolare dell'azienda effettua una valutazione dell'evento per la corretta analisi della situazione.

Sulla scorta delle determinazioni raggiunte, il titolare dell'azienda predispone l'eventuale comunicazione all'Autorità Garante, a firma del Titolare del trattamento, da inviare senza ingiustificato ritardo e, ove possibile, entro 72 ore, da determinarsi dal momento in cui il Titolare del trattamento ne è venuto a conoscenza, cioè quando abbia un ragionevole grado di certezza della verificazione di un incidente di sicurezza che riguardi dati personali. Vedi **allegato Modello di Notifica Garante (Data Breach).**

Oltre il termine delle 72 ore, la notifica deve essere corredata delle ragioni del ritardo.

È comunque fatta salva la possibilità di fornire successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla violazione di cui il titolare del trattamento venga a conoscenza, a seguito della effettuazione di ulteriori indagini e attività di follow-up (c.d. notifica in fasi)

La scelta e le motivazioni che hanno portato a non notificare l'evento deve essere documentata a cura del titolare dell'azienda.

### 2.3.5 *Modalità di Comunicazione agli interessati*

Nel caso in cui dal data breach possa derivare un rischio elevato per i diritti e le libertà delle persone, anche queste devono essere informate senza ingiustificato ritardo, al fine di consentire loro di prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione.

La comunicazione all'interessato descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d) del Regolamento UE n. 2016/679.

Il titolare dell'azienda predispone l'eventuale comunicazione all'interessato/agli interessati, a firma del Titolare del trattamento, da inviarsi nei tempi e nei modi che lo stesso individuerà come più opportuna come specificato nell'art. 34 del GDPR e tenendo conto di eventuali indicazioni fornite dall'Autorità Garante.

Non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

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

Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 dell'art.34 del citato Regolamento è soddisfatta.

# 3 ISTRUZIONI

## 3.1 IO-01 ISTRUZIONI RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI

### *3.1.1 SCOPO DELL'ISTRUZIONE OPERATIVA*

In ottemperanza alle disposizioni del ***Regolamento UE 679/2016*** ed in relazione alle attività svolte nell'ambito dell'Azienda, il **"RESPONSABILE ESTERNO AL TRATTAMENTO DEI DATI"** è la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento. Egli deve possedere l'abilità e l'affidabilità per assicurare la completa conformità con le disposizioni di legge in materia di trattamento di dati personali, con particolare riferimento alle misure di sicurezza.

**Compito specifico del titolare del trattamento è quello di valutare il rischio del trattamento** che pone in essere tramite i responsabili. Il titolare del trattamento deve sempre poter sindacare le decisioni dei responsabili.

**Il Responsabile Esterno Trattamento, secondo il Regolamento europeo, è riservato ad un soggetto esterno all'azienda.**

### *3.1.2 RESPONSABILITÀ*

Nel caso di trattamento in violazione delle norme del regolamento europeo, il responsabile esterno del trattamento risponde, congiuntamente al titolare del trattamento, per il danno cagionato all'interessato, secondo quanto previsto dall'articolo 82 e dal Considerando 28.

Il responsabile esterno del trattamento risponde per il danno causato dal trattamento solo in caso di non corretto adempimento degli obblighi previsti dalle norme in capo al responsabile stesso, oppure se ha agito in modo difforme rispetto alle istruzioni del titolare del trattamento.

Egli si fa carico di rispettare e di far rispettare ai propri dipendenti e a qualsiasi altra persona (consulenti, subappaltatori, ecc.) deputata a trattare dati personali forniti dal Titolare del trattamento, le istruzioni di seguito descritte e qualsiasi altra istruzione scritta, comunicata dal Titolare del trattamento.

Tali istruzioni sono soggette ad aggiornamenti, modifiche e/o integrazioni in accordo con le disposizioni di qualsiasi legge sulla privacy applicabile che sarà implementata nel corso di validità della nomina.

### *3.1.3 MODALITÀ OPERATIVE*

I Responsabile esterno al trattamento dei dati personali, deve scrupolosamente attenersi alle istruzioni dettate dal Titolare del Trattamento e devono essere considerate ordine di servizio.

#### *3.1.3.1 Principi generali da osservare*

Ogni trattamento di dati personali deve avvenire, nel rispetto primario dei seguenti principi di ordine generale:

Ai sensi dell'art.5 del Reg. UE 679/16, che prescrive i 'Principi applicabili al trattamento di dati personali" per ciascun trattamento di propria competenza, il Responsabile esterno del trattamento deve fare in modo che siano sempre rispettati i seguenti presupposti:

I dati devono essere trattati:

secondo il **principio di liceità**, vale a dire conformemente alle disposizioni del Regolamento, nonché alle disposizioni del Codice Civile, per cui, più in particolare, il trattamento non deve essere contrario a norme imperative, all'ordine pubblico ed al buon costume;
secondo il **principio fondamentale di correttezza**, il quale deve ispirare chiunque tratti qualcosa che appartiene alla sfera altrui;
secondo il **principio di trasparenza**, che consente all'interessato di venire a conoscenza delle metodologie e delle finalità di utilizzo dei propri dati;
secondo il **principio di adeguatezza** il trattamento dei dati deve essere riferibile alla tipologia di incarico o mansione svolta;
secondo il **principio di pertinenza**, ovvero, i dati devono essere trattati in relazione allo scopo a cui sono destinati;
secondo il principio della limitatezza, la raccolta dei dati non può eccedere ai dati strettamente necessari per la finalità perseguita.
I dati devono essere raccolti solo per scopi:

**esatti,** cioè, precisi e rispondenti al vero e, se necessario, aggiornati;
**conservati** per un periodo non superiore a quello necessario per gli scopi del trattamento e comunque in base alle disposizioni aventi ad oggetto le modalità ed i. tempi di conservazione degli atti amministrativi. Trascorso, detto periodo i dati vanno resi anonimi o cancellati la loro comunicazione diffusione non è più consentita.
Trattati in modo tale che venga garantita **un'adeguata sicurezza** dei dati personali mediante misure tecniche ed organizzative adeguate;
**determinati,** vale a dire che non è consentita la raccolta come attività fine a sé stessa;
**espliciti**, nel senso che il soggetto interessato va informato sulle finalità del trattamento;
**legittimi**, cioè, oltre al trattamento, come è evidente, anche il fine della raccolta dei dati deve essere lecito.
Ciascun trattamento deve, inoltre, avvenire nei limiti imposti dal principio fondamentale di riservatezza e nel rispetto della dignità della persona dell'interessato al trattamento, ovvero deve essere effettuato eliminando ogni occasione di impropria conoscibilità dei dati da parte di terzi.

#### *3.1.3.2 Violazioni*

Per la violazione delle disposizioni di cui al Regolamento Europeo in materia di trattamento dei dati personali sono previste **sanzioni amministrative e pecuniarie** (art. 83). Per le altre sanzioni riferibili alle violazioni non soggette amministrative e pecuniarie si rimanda alla legislazione nazionale.

In ogni caso, la **responsabilità penale** per eventuale uso non corretto dei dati oggetto di tutela, resta a carico della singola persona cui l'uso illegittimo degli stessi sia imputabile.

Mentre, in merito alla **responsabilità civile**, si fa rinvio all'art.2050 del Codice Civile, che dispone relativamente ai danni cagionati per effetto del trattamento ed ai conseguenti obblighi di risarcimento, implicando, a livello pratico, che, per evitare ogni responsabilità, l'operatore è tenuto a fornite prova di avere applicato le misure tecniche di sicurezza più idonee a garantire appunto la sicurezza dei dati detenuti.

### *3.1.4 COMPITI PARTICOLARI DEL RESPONSABILE ESTERNO DEL TRATTAMENTO*

**L'addetto esterno** al trattamento dei dati personali, operando nell'ambito dei principi sopra ricordati, deve attenersi ai seguenti compiti di carattere particolare:

- ✓ identificare e censire i trattamenti di dati personali, le banche dati e gli archivi gestiti con supporti informatici e/o cartacei necessari all'espletamento delle attività istituzionalmente rientranti nella propria sfera di competenza;
- ✓ definire, per ciascun trattamento di dati personali, la durata del trattamento e la cancellazione o anonimizzazione dei dati obsoleti, nel rispetto della normativa vigente in materia di prescrizione e tenuta archivi;
- ✓ ogni qualvolta si raccolgano dati personali, provvedere a che venga fornita l'informativa ai soggetti interessati, ai sensi dell'artt.13 – 14 –21del Regolamento;
- ✓ adempiere agli obblighi di sicurezza, quali attenersi alle disposizioni di cui agli artt.25 e 32 del Regolamento, cioè adottare le misure di sicurezza idonee adottare tutte le preventive misure di Sicurezza ritenute idonee al fine di ridurre al minimo il rischio di distruzione o perdita anche accidentale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- ✓ comunicare tempestivamente al Titolare del trattamento casi di accesso non autorizzato ai dati o di trattamento non consentito o non conforme alle finalità perseguite;
- ✓ far osservare gli adempimenti previsti in caso di nuovi trattamenti e cancellazione di trattamenti;
- ✓ segnalare al Titolare del trattamento l'eventuale cessazione di trattamento.

In merito agli addetti, il **Responsabile Esterno del trattamento** deve:

- ✓ individuare, trai propri collaboratori, designandoli per iscritto, addetti al trattamento fornendo loro le istruzioni a cui devono attenersi per svolgere le operazioni di trattamento;
- ✓ adoperarsi al fine di rendere effettive le suddette istruzioni cui devono attenersi gli addetti del trattamento, curando in particolare il profilo della riservatezza, della sicurezza di accesso e della integrità dei dati e l'osservanza parte degli addetti, nel compimento delle operazioni di trattamento, dei principi di carattere generale che informano la vigente disciplina in materia;
- ✓ stabilire le modalità di accesso ai dati e l'organizzazione del lavoro degli addetti, avendo cura di adottare preventivamente le misure organizzative idonee e impartite le necessarie istruzioni ai fini di riscontro di eventuali richieste di esecuzione dei diritti di cui all'art.5, agli artt. 12 e ss. Fino al 22 e all'art. 34;
- ✓ evadere le eventuali richieste di accesso, rettifica, integrazione, cancellazione, blocco dei dati da parte dell'interessato che eserciti i propri diritti ai sensi degli artt. di cui sopra;
- ✓ collaborare con il Titolare del trattamento all'adempimento degli obblighi previsti dal Regolamento e segnalare eventuali problemi applicativi.

## 3.2 IO-02 ISTRUZIONI AGLI INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI COMUNI, SENSIBILI E/O GIUDIZIARI

### *3.2.1 Scopo dell'istruzione operativa*

In ottemperanza alle disposizioni del ***Regolamento UE 679/2016*** ed in relazione alle attività svolte nell'ambito dell'Azienda, l'"**INCARICATO**", dovrà effettuare i trattamenti di dati personali di competenza attenendosi scrupolosamente alle seguenti istruzioni e ad ogni ulteriore indicazione, anche verbale, che potrà essere fornita dal "Responsabile esterno del trattamento".

I dati personali devono essere trattati:

e. in osservanza dei criteri di riservatezza;
f. *in modo lecito e secondo correttezza;*
g. *per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati;*
h. *nel pieno rispetto delle misure di sicurezza, custodendo e controllando i dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.*

Le misure di sicurezza sono obbligatorie e sono distinte in funzione delle seguenti modalità di trattamento dei dati:

13. **senza l'ausilio di strumenti elettronici** (es. dati in archivi cartacei o su supporto magnetico/ottico);
14. **con strumenti elettronici** (PC ed elaboratori).

### *3.2.2 Trattamenti senza l'ausilio di strumenti elettronici*

I dati personali archiviati su supporti di tipo magnetico e/o ottico devono essere protetti con le stesse misure di sicurezza previste per i supporti cartacei.

Le misure di sicurezza applicate alle copie o alle riproduzioni dei documenti contenenti dati personali devono essere identiche a quelle applicate agli originali.

#### *3.2.2.1 Custodia*

- ✓ I documenti contenenti dati personali, devono essere custoditi in modo da non essere accessibili a persone non incaricate del trattamento (es. armadi o cassetti chiusi a chiave).
- ✓ I documenti contenenti dati personali che vengono prelevati dagli archivi per l'attività quotidiana devono esservi riposti a fine giornata.
- ✓ I documenti contenenti dati personali non devono rimanere incustoditi su scrivanie o tavoli di lavoro.

#### *3.2.2.2 Comunicazione*

- ✓ L'utilizzo dei dati personali deve avvenire in base al principio del "need to know" e cioè essi non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative (anche se queste persone sono a loro volta incaricate del trattamento).
- ✓ I dati non devono essere comunicati all'esterno e comunque a soggetti terzi se non previa autorizzazione.

#### *3.2.2.3 Distruzione*

- ✓ Qualora sia necessario distruggere i documenti contenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere sminuzzati in modo da non essere più ricomponibili.
- ✓ I supporti magnetici od ottici contenenti dati personali devono essere cancellati prima di essere riutilizzati. Se ciò non è possibile, essi devono essere distrutti.

#### 3.2.2.4 *Ulteriori istruzioni in caso di trattamento di dati sensibili e/o giudiziari*

- ✓ I documenti contenenti dati sensibili e/o giudiziari devono essere controllati e custoditi dagli Incaricati in modo che non vi accedano persone prive di autorizzazione.
- ✓ L'archiviazione dei documenti cartacei contenenti dati sensibili e/o giudiziari deve avvenire in locali ad accesso controllato, utilizzando armadi o cassetti chiusi a chiave.
- ✓ Per accedere agli archivi contenenti dati sensibili e/o giudiziari fuori orario di lavoro è necessario ottenere una preventiva autorizzazione da parte del Responsabile esterno del trattamento.

### 3.2.3 *Trattamenti con strumenti elettronici*

#### 3.2.3.1 *Gestione delle credenziali di autenticazione*

La legge prevede che l'accesso alle procedure informatiche che trattano dati personali sia consentito agli Incaricati in possesso di "***credenziali di autenticazione***" che permettano il superamento di una procedura di autenticazione.

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'Incaricato (User-id) associato ad una parola chiave riservata (password).

Gli Incaricati devono utilizzare e gestire le proprie credenziali di autenticazione attenendosi alle seguenti istruzioni.

- ✓ Le **user-id individuali** per l'accesso alle applicazioni non devono mai essere condivise tra più utenti (anche se Incaricati del trattamento). Nel caso altri utenti debbano poter accedere ai dati è necessario richiedere l'autorizzazione al Responsabile esterno del trattamento.
- ✓ Gli **strumenti di autenticazione** (ad esempio le **password**) che consentono l'accesso alle applicazioni devono essere mantenute riservate. Essi non vanno mai condivisi con altri utenti (anche se Incaricati del trattamento).
- ✓ Le **password** devono essere sostituite almeno ogni sei mesi.
- ✓ Le **password** devono essere composte da almeno 8 caratteri alfanumerici.

#### 3.2.3.2 *Protezione del pc e dei dati*

- ✓ Tutti i PC devono essere dotati di software antivirus aggiornato costantemente e con la funzione "Monitor" attiva.
- ✓ Per evitare accessi illeciti, deve essere sempre attivato il salva schermo con password.
- ✓ Sui PC devono essere installati, appena vengono resi disponibili (e comunque almeno annualmente), tutti gli aggiornamenti software necessari a prevenirne vulnerabilità e correggerne i difetti.
- ✓ Deve essere effettuato, con cadenza minima semestrale un salvataggio con creazione di uno *snapshot* del PC personale.

3.2.3.2.1 Cancellazione dei dati dal pc

- ✓ I dati personali conservati sui PC devono essere cancellati in modo sicuro (es. formattando i dischi) prima di destinare i PC ad usi diversi.

3.2.3.2.2 Ulteriori istruzioni in caso di trattamento di dati sensibili e/o giudiziari

- ✓ Le password di accesso alle procedure informatiche che trattano dati sensibili e/o giudiziari devono essere sostituite almeno ogni sei mesi.

- ✓ L'installazione degli aggiornamenti software necessari a prevenire vulnerabilità e correggerne i difetti dei programmi per elaboratori deve essere effettuata almeno semestralmente.

### *3.2.4 Istruzioni di carattere generale*

**Come scegliere e usare la password:**

- ✓ Usare almeno 8 caratteri alfanumerici;
- ✓ Non utilizzare date di nascita, nomi o cognomi propri o di parenti;
- ✓ Non sceglierla uguale alla matricola o alla user-id
- ✓ Custodirla sempre in un luogo sicuro e non accessibile a terzi
- ✓ Non divulgarla a terzi
- ✓ Non condividerla con altri utenti

**Come comportarsi in presenza di ospiti o di personale di servizio:**

- ✓ Fare attendere gli ospiti in luoghi in cui non siano presenti informazioni riservate o dati personali.
- ✓ Se è necessario allontanarsi dalla scrivania in presenza di ospiti, riporre i documenti e attivare il salvaschermo del PC.
- ✓ Non rivelare o fare digitare le password dal personale di assistenza tecnica.
- ✓ Non rivelare le password al telefono né inviarla via fax -nessuno è autorizzato a chiederle.
- ✓ Segnalare qualsiasi anomalia o stranezza al Responsabile esterno del trattamento.

**Come gestire la posta elettronica:**

- ✓ Non aprire messaggi con allegati di cui non si conoscono l'origine, possono contenere virus in grado di cancellare i dati sul PC.
- ✓ Evitare di aprire filmati e presentazioni non attinenti all'attività lavorativa per evitare situazioni di pericolo per i dati contenuti sul vostro PC.

**Come usare correttamente Internet:**

- ✓ Evitare di scaricare dalla rete file e software di uso non direttamente riferibile all'attività di lavoro, in quanto questo può essere pericoloso per i dati e la rete dell'Azienda.
- ✓ Usare Internet solo per lavoro, i siti web spesso nascondono insidie per i visitatori meno esperti.
- ✓ Non leggere le caselle personali esterne via webmail in quanto alcuni provider esterni non proteggono dai virus.

## 3.3 IO-03 ISTRUZIONI AGLI AMMINISTRATORI DI SISTEMA

### *3.3.1 Scopo dell'istruzione operativa*

In ottemperanza alle disposizioni del ***Regolamento UE 679/2016*** ed in relazione alle attività svolte nell'ambito dell'Azienda, l'"**AMMINISTRATORE DI SISTEMA**", ossia colui che *è preposto*

*alla sicurezza, alla gestione e alla manutenzione delle banche dati, dei sistemi e delle infrastrutture informatiche di un'Azienda*. Ad essi vengono associati anche gli amministratori di reti e gli amministratori di sistemi software complessi che, in ragione delle proprie mansioni, come ad esempio, attività tecniche quali il salvataggio dei dati (*backup/recovery*), l'organizzazione dei flussi di rete, la gestione dei supporti di

memorizzazione e manutenzione *hardware*, possono avere il privilegio di accedere ai dati personali trattati dal titolare del trattamento.

Gli **Amministratori di Sistema** *sono tenuti ad adottare idonee misure volte a prevenire e ad accertare eventuali accessi non consentiti ai dati personali, in particolare quelli commessi con abuso della qualità di amministratore di sistema*. A tal proposito viene posta attenzione anche alla necessità di valutare attentamente le caratteristiche soggettive, di condotta, affidabilità e professionalità dei soggetti cui attribuire tale ruolo.

***Tale figura, inoltre, è tenuta anche al pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati, in quanto il più delle volte viene definito come "incaricato al trattamento".***

### 3.3.2 Modalità di trattamento

L'**Amministratore di Sistema** dovrà attenersi scrupolosamente alle seguenti istruzioni:

- ✓ generare, sostituire ed invalidare, in relazione agli strumenti ed alle applicazioni informatiche utilizzate, le parole chiave ed i Codici identificativi personali da assegnare agli incaricati del trattamento dati, svolgendo anche la funzione di custode delle copie;
- ✓ procedere, più in particolare, alla disattivazione dei Codici identificativi personali, in caso di perdita della qualità che consentiva all'utente o incaricato l'accesso all'elaboratore;
- ✓ adottare adeguati programmi antivirus, firewall ed altri strumenti software o hardware atti a garantire la massima misura di sicurezza ed utilizzando le conoscenze acquisite in base al progresso tecnico software e hardware, verificandone la corretta installazione, i costanti aggiornamenti e il totale funzionamento degli stessi;
- ✓ adottare tutti i provvedimenti necessari ad evitare la perdita o la distruzione, anche solo accidentale, dei dati personali e provvedere al ricovero periodico degli stessi con copie di backup, vigilando sulle procedure attivate in struttura. L'amministratore di sistema dovrà anche assicurarsi della qualità delle copie di backup e della loro conservazione in luogo adeguato e sicuro;
- ✓ indicare al personale competente o prevedere direttamente alla distruzione e smaltimento dei supporti informatici di memorizzazione logica o alla cancellazione dei dati per il loro reimpiego;
- ✓ vigilare sugli interventi informatici diretti al sistema informatico della società, effettuati da operatori esterni. In caso di anomalie sarà sua cura segnalarle direttamente alla direzione;
- ✓ monitorare le eventuali ulteriori misure di sicurezza per il trattamento informatico dei dati sensibili (se esistenti e giudiziari) e per la conseguente tutela degli strumenti elettronici;
- ✓ adottare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici;
- ✓ le registrazioni (access log) comprendono i riferimenti temporali e la descrizione dell'evento che le ha generate ed hanno caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste. In ogni caso è tassativamente vietato intervenire in alcun modo su di esse (ad es. cancellandole, modificandole, alterandole, ecc. o compiendo qualsiasi altra attività sulle stesse).
- ✓ le registrazioni sono conservate nel rispetto dei termini previsti nelle finalità del rapporto;

- ✓ l'operato del designato sarà oggetto, con cadenza almeno annuale, di un'attività di verifica da parte del Titolare del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti;
- ✓ deve prestare particolare cura al rispetto delle misure di sicurezza dei dati, adottate per il trattamento dei dati con strumenti elettronici o senza. Deve quindi applicare le misure di sicurezza al fine di garantire il corretto funzionamento di esse anche con riferimento agli strumenti elettronici affidati per i quali svolge attività di manutenzione, assistenza, sviluppo, ecc.
- ✓ l'amministratore di sistema può trattare i soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati e/o comunque i soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di trattamento e per svolgere le attività attribuite e le mansioni di competenza;
- ✓ deve rispettare le norme sul trattamento dei dati personali ed in particolare, per quanto di competenza, anche quelle in materia di informazioni da fornire, quelle sul consenso da richiedere (laddove applicabili), tenendo presente che i dati personali debbono essere trattati in modo lecito e secondo correttezza, per scopi determinati, espliciti e legittimi. I dati debbono essere esatti e, se necessario, aggiornati, pertinenti, completi e non eccedenti rispetto alle finalità e conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi;
- ✓ gli atti e i documenti contenenti i dati devono essere conservati in archivi ad accesso selezionato e, quando affidati al designato, devono essere da quest'ultimo conservati (con conseguente obbligo di custodia degli stessi) e restituiti al termine delle operazioni affidate;
- ✓ in caso di allontanamenti, anche momentanei, dall'ufficio debbono essere adottate le misure e precauzioni del caso rispetto ad accessi illeciti o comunque non autorizzati.
- ✓ a conclusione dell'attività lavorativa le misure e precauzioni adottate dovranno essere in ogni caso conformi a quanto previsto dalle norme e da regolamenti aziendali, procedure e policy, e, comunque, adeguate alla durata dell'interruzione;
- ✓ deve essere controllata l'integrità dei dati stessi.

# 4 CODICE DI CONDOTTA

Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016.

L'AZIENDA non ha ritenuto di dover aderire ad alcun codice di condotta. Ha però adottato, in applicazione della normativa di settore, il Modello di Organizzazione, Gestione e Controllo, ai sensi e per gli effetti della Legge n. 231/2001 e ss.mm.ii..

## 4.1 OBIETTIVO

L'obiettivo del **codice di condotta** consiste nello stabilire standard di protezione sicurezza uniformi, adeguati e globali all'interno dell'Azienda, allo scopo di soddisfare i requisiti fissati dalle normative vigenti.

Il **codice di condotta** crea in questo contesto un livello di protezione dei dati uniforme a livello di tutta l'azienda, senza sostituire la legittimazione che deve essere alla base di qualsiasi elaborazione o trasmissione di dati.

## 4.2 LIMITI DI VALIDITÀ

Il **codice di condotta** è una direttiva aziendale valida per il trattamento di qualunque dato necessario alla gestione delle procedure aziendali.

## 4.3 PRINCIPI PER L'ELABORAZIONE DEI DATI PERSONALI

Nell'elaborazione dei dati è necessario tutelare i diritti personali alla privacy degli interessati.

I dati personali possono essere elaborati esclusivamente se ciò risulta legalmente ammissibile o se il soggetto interessato ha fornito il proprio consenso e possono essere elaborati esclusivamente ai fini per i quali sono stati originariamente raccolti.

I dati personali devono essere memorizzati correttamente e, qualora necessario, periodicamente aggiornati. A tale scopo occorre adottare provvedimenti idonei per cancellare o rettificare i dati che risultano incorretti o incompleti.

Ai dati personali possono accedere soltanto i dipendenti che operano in un settore di attività connesso al trattamento di tali dati: l'autorizzazione all'accesso deve essere limitata in base al tipo e alla portata della rispettiva area di competenza.

I dati personali che non risultano più necessari ai fini per i quali sono stati originariamente raccolti e memorizzati, devono essere cancellati in conformità con le norme vigenti sulla conservazione dei dati.

Qualora l'interessato si sia opposto all'utilizzo dei propri dati personali a scopo di marketing, i dati non potranno essere utilizzati a tal fine.

Il trattamento dei dati deve essere finalizzato allo scopo di rilevare, elaborare e utilizzare esclusivamente i dati personali necessari, ovvero la minima quantità possibile di informazioni. Le possibilità di anonimizzazione e pseudonimizzazione sono ammesse, laddove ciò sia possibile e gli oneri di queste procedure risultino adeguatamente rapportati alle finalità di protezione dei dati che si intende perseguire. Le valutazioni statistiche

o le analisi effettuate sulla base di dati anonimizzati o pseudonimizzati non sono rilevanti ai fini della protezione dei dati personali, in quanto tali dati non risultano più individualizzabili.

Nei progetti di elaborazione dei dati dai quali possono derivare particolari rischi per la tutela del diritto alla privacy degli interessati, il Responsabile esterno del trattamento dei dati deve essere interpellato a partire dalle prime fasi del processo di elaborazione.

Quanto sopra vale in particolare per le tipologie di dati personali elencate qui di seguito.

## 4.4 TIPOLOGIE PARTICOLARI DI DATI PERSONALI

L'elaborazione dei dati personali relativi alla provenienza razziale ed etnica, alle opinioni politiche, alle convinzioni religiose o filosofiche, all'appartenenza a sindacati oppure sulla salute o sull'orientamento sessuale dell'interessato è generalmente vietata, salvo che:

n) la legittimità dell'elaborazione non derivi da un'autorizzazione legale o da un requisito di legge;
o) 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;
p) 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;
q) 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;
r) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
s) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali (l'elaborazione di questo genere di dati personali, inoltre, è consentita per la convalida, l'esercizio o la tutela di diritti legali anche nell'ambito di una controversia giudiziaria, qualora non sussista alcun motivo per supporre che prevalga il legittimo interesse dell'interessato all'esclusione dell'elaborazione o dell'utilizzo dei dati).
t) 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;
u) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3 del Regolamento UE n. 2016/679;
v) 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;

w) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, Regolamento UE n. 2016/679, 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;

In tutti gli altri casi, l'interessato deve avere fornito espressamente il proprio consenso all'elaborazione di questi dati.

Da ultimo, i dati personali di categorie particolari possono essere trattati per le finalità di cui alla lettera h), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti.

Quanto, invece, al trattamento dei dati personali relativi a condanne penali e reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, del Regolamento UE N. 2016/679, 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. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.

Se le finalità per cui un titolare del trattamento tratta i dati personali non richiedono o non richiedono più l'identificazione dell'interessato, il titolare del trattamento non è obbligato a conservare, acquisire o trattare ulteriori informazioni per identificare l'interessato al solo fine di rispettare il presente regolamento.

Qualora, in quest'ultima circostanza, il titolare del trattamento possa dimostrare di non essere in grado di identificare l'interessato, ne informa l'interessato, se possibile. In tali casi, gli articoli da 15 a 20 del Regolamento UE n. 2016/679, non si applicano tranne quando l'interessato, al fine di esercitare i diritti di cui ai suddetti articoli, fornisce ulteriori informazioni che ne consentano l'identificazione.

## 4.5 INFORMAZIONE E CONSENSO DELL'INTERESSATO

I dati personali dell'interessato possono essere rilevati ed elaborati sulla base e ai fini di esecuzione del contratto e dell'avviamento del rapporto di lavoro. In questo contesto sono consentiti anche l'elaborazione e l'utilizzo a fine di marketing o di ricerche di mercato e sondaggi di opinione, nella misura in cui ciò risulti in accordo con lo scopo per i quali i dati sono stati originariamente rilevati.

Al momento del rilevamento dei dati personali presso l'interessato, salvo che quest'ultimo disponga già di tutte le informazioni, l'interessato deve essere consapevole o informato di quanto segue:

- ✓ l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
- ✓ le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento,
- ✓ i legittimi interessi perseguiti dal titolare del trattamento o da terzi, qualora il trattamento si basi 6, paragrafo 1, lettera f) del Regolamento UE n. 2016/679;
- ✓ gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali.
- ✓ ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, paragrafo 1, secondo comma, del detto Regolamento, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili.

Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 del Regolamento UE n. 2016/679 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

Nel momento in cui i dati personali sono ottenuti, il *titolare del trattamento* fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:

- ✓ il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- ✓ l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
- ✓ l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la *liceità del trattamento* basata sul consenso prestato prima della revoca;
- ✓ qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a) del detto Regolamento, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- ✓ il diritto di proporre reclamo a un'autorità di controllo se la comunicazione di dati personali è un obbligo legale o contrattuale, oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
- ✓ l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

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

Il titolare del trattamento fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta ai sensi degli articoli da 15 a 22 del Regolamento UE n. 2016/679 senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Il titolare del trattamento informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta. Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato.

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

Le informazioni fornite ai sensi degli articoli 13 e 14 ed eventuali comunicazioni e azioni intraprese ai sensi degli articoli da 15 a 22 e dell'articolo 34 del Regolamento UE n. 2016/679 sono gratuite. Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento può:

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

b) rifiutare di soddisfare la richiesta.

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

Qualora il titolare del trattamento nutra ragionevoli dubbi circa l'identità della persona fisica che presenta la richiesta di cui agli articoli da 15 a 21 del detto Regolamento, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato, salvo che si tratti di un trattamento che non richiede l'identificazione (art. 11 Regolamento UE n. 2016/679).

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

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

- ✓ l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
- ✓ le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- ✓ le categorie di dati personali in questione;
- ✓ gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- ✓ l'eventuale intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale, l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, paragrafo 1, secondo comma, del Regolamento UE 2016/679, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili.

Il *titolare del trattamento* fornisce all'interessato anche le seguenti informazioni necessarie per garantire un trattamento corretto e trasparente nei confronti dell'interessato:

- ✓ il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- ✓ i legittimi interessi perseguiti dal titolare del trattamento o da terzi. Tale comunicazione deve avvenire solo nel caso in cui 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.
- ✓ l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
- ✓ solo ove l'interessato abbia espresso il consenso al trattamento dei dati personali per una o più specifiche finalità o nel caso di categorie particolari di dati di cui all'art. 9, paragrafo 2, lettera a, del Regolamento UE 2016/679, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- ✓ il diritto di proporre reclamo a un'autorità di controllo, la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;
- ✓ l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato. Questa trasparenza può essere assicurata mediante una comunicazione individuale od informazioni fornite a carattere generale. Qualora non sussista un rapporto contrattuale, l'interessato deve avere acconsentito al rilevamento e all'elaborazione dei propri dati personali, a

meno che l'ammissibilità del rilevamento e dell'elaborazione non sia fondata sulle norme del diritto nazionale. Quanto sopra vale anche nel caso in cui si debba procedere a un'ulteriore elaborazione o al successivo trattamento dei dati per motivi che esulano dai fini originari del rilevamento.

Il titolare del trattamento fornisce le dette informazioni:

a) entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;
b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; oppure
c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.

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

I suesposti adempimenti non si attuano nella misura in cui:

a) l'interessato dispone già delle informazioni;
b) comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1, del Regolamento UE n. 2016/679, o nella misura in cui l'obbligo di cui al paragrafo 1 dell'art. 14 del detto Regolamento, rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni;
c) l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato; oppure
d) qualora i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri, compreso un obbligo di segretezza previsto per legge.

Prima di rilasciare il consenso, l'**interessato** deve essere informato.

La **dichiarazione di consenso**, per esigenze probatorie, deve essere regolarmente rilasciata per iscritto. Nella dichiarazione di consenso devono essere specificati l'entità e lo scopo della procedura di elaborazione dei dati.

Di norma, i dati personali devono essere rilevati direttamente dall'interessato. Qualora i dati vengano raccolti presso terzi o trasmessi da terzi, è necessario verificare che alla prima richiesta dei dati l'interessato sia stato o venga conformemente informato.

## 4.6 DIRITTI DEGLI INTERESSATI

Per eventuali chiarimenti e reclami, gli interessati possono rivolgersi al *titolare del trattamento* in persona del legale rappresentante. In particolare, qualora gli interessati intendano esercitare i diritti elencati in seguito, le richieste in tal senso devono essere immediatamente evase.

L'**interessato** può chiedere informazioni in merito al contenuto dei dati personali memorizzati sul suo conto, alla loro provenienza e allo scopo per il quale sono stati archiviati.

In caso di trasmissione di dati personali a terzi, è necessario fornire informazioni anche sull'identità dei destinatari o sulle categorie di destinatari dei dati.

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

a) le finalità del trattamento
b) le categorie di dati personali in questione;
c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
f) il diritto di proporre reclamo a un'autorità di controllo;
g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, del Regolamento UE n. 2016/679, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 del detto Regolamento relative al trasferimento.

Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

Il diritto di ottenere una copia non deve ledere i diritti e le libertà altrui.

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

Qualora, per esempio nell'ambito dell'esercizio *del diritto di informazione*, si dovesse riscontrare che i dati personali risultano inesatti o incompleti, **l'interessato ha il diritto di esigere una correzione.**

Laddove dovesse risultare che lo scopo dell'elaborazione dei dati sia venuto meno per decorrenza dei termini o per altri motivi, oppure il trattamento dei dati sia illegale e questo finora sia stato ignorato nell'ambito delle verifiche periodiche, i dati dovranno essere cancellati, tenendo eventualmente conto degli obblighi di legge sulla conservazione delle informazioni.

L'**interessato** ha il *diritto di rifiutare il suo consenso all'utilizzo dei propri dati personali* ai fini di pubblicità diretta, oppure di ricerche di mercato o sondaggi di opinione. L'utilizzo dei dati a tali scopi deve essere pertanto interdetto.

Inoltre, l'**interessato** ha il diritto fondamentale di rifiutare il proprio consenso all'elaborazione dei propri dati personali, del quale va tenuto conto nel caso in cui una verifica determini che il suo legittimo interesse, a causa di una particolare situazione, prevalga sull'interesse dell'ufficio responsabile.

Quanto sopra non è valido nel caso in cui una norma di legge prescriva l'obbligo di elaborazione o di utilizzo dei dati.

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

- ✓ *i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;*
- ✓ *l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a) del Regolamento UE n. 2016/679 e se non sussiste altro fondamento giuridico per il trattamento;*
- ✓ *l'interessato si oppone al trattamento, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento oppure si oppone al trattamento per finalità di marketing;*
- ✓ *i dati personali sono stati trattati illecitamente;*
- ✓ *i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione europea o dello stato membro cui è soggetto il titolare del trattamento;*
- ✓ *i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1, del Regolamento UE n. 2016/679;*

I detti adempimenti non si attuano nella misura in cui il trattamento sia necessario:

a) per l'esercizio del diritto alla libertà di espressione e di informazione;
b) per l'adempimento di un obbligo giuridico che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3, del detto Regolamento;
d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, del detto Regolamento, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;
e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

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

L'**interessato** ha il diritto di ottenere dal titolare del trattamento la *limitazione* del trattamento quando ricorre una delle seguenti ipotesi:

- ✓ l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;
- ✓ il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo benché il titolare del trattamento non ne abbia più bisogno ai fini del

trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;

- ✓ l'interessato si è opposto al trattamento, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

Se il trattamento è limitato, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

L'interessato che ha ottenuto la limitazione del trattamento è informato dal titolare del trattamento prima che detta limitazione sia revocata.

Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali *rettifiche o cancellazioni* o limitazioni del trattamento effettuate a norma dell'articolo 16, dell'articolo 17, paragrafo 1, e dell'articolo 18, del Regolamento UE n. 2016/679, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

L'**interessato** ha il diritto di esercitare il *diritto alla portabilità dei dati* ovvero ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora il trattamento si basi sul consenso o su un contratto e il trattamento sia effettuato con mezzi automatizzati.

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

L'esercizio del diritto alla portabilità dei dati lascia impregiudicato l'articolo 17 del Regolamento UE n. 2016/679 e non deve ledere i diritti e le libertà altrui.Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

Nell'ambito dell'esercizio *del diritto di opposizione*, l'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), del detto Regolamento, compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

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

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

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

Nel contesto dell'utilizzo di servizi della società dell'informazione e fatta salva la direttiva 2002/58/CE (Direttiva del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.

Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1, del Regolamento UE n. 2016/679, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguardano, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

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

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

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

Le decisioni non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del Regolamento UE n. 2016/679, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), del detto Regolamento, e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

L'AZIENDA ha adottato, in data 03.11.2023, un'apposita procedura di per la gestione delle richieste di esercizio dei diritti degli interessati, ai sensi e per gli effetti degli artt. 15 - 22 del Regolamento UE 2016/679 (GDPR) (**Vedi allegato procedura di per la gestione delle richieste di esercizio dei diritti degli interessati**)

## 4.7 SEGRETEZZA DEL PROCESSO DI ELABORAZIONE

Esclusivamente i dipendenti autorizzati ed espressamente vincolati all'*obbligo di segretezza* sul contenuto dei dati possono raccogliere, elaborare o utilizzare le informazioni personali.

In particolare, è vietato sfruttare questi dati a fini privati, trasmettere le informazioni a persone non autorizzate o comunque renderle accessibili a queste ultime in altro modo.

L'obbligo di segretezza permane anche dopo la conclusione del rapporto di lavoro.

## 4.8 PRINCIPI DI SICUREZZA DEI DATI

Le *misure tecniche e organizzative* necessarie per garantire la sicurezza dei dati si riferiscono a:

elaboratori (server e workstation),

reti o connessioni per la comunicazione in rete, applicazioni,

addetti alla gestione dei dati personali.

Per quanto concerne i **server**, sono previste misure di sicurezza fisiche e infrastrutturali che comprendono i controlli di accesso (con livelli di autorizzazione differenziati), sistemi di chiusura e dispositivi antincendio.

Tutte le **workstation** sono dotate di un sistema di protezione mediante password.

La rete aziendale è protetta da sistemi firewall contro i tentativi di accesso dall'esterno non autorizzati e di intromissioni da Internet.

Al fine di proteggere i dati personali contenuti nelle banche dati, è previsto un sistema di accesso e di intervento riferito al nominativo personale e al tipo di applicazione.

Per ciò che attiene il personale che gestisce i dati lo stesso è stato adeguatamente formato per una corretta gestione dei dati ai sensi del disciplinare tecnico in materia di misure minime di sicurezza.

Le suddette misure tecnico-organizzative sono integrate in un sistema di gestione della tutela e sicurezza dei dati che presiede alle diverse responsabilità.

## 4.9 PROVVEDIMENTI, SANZIONI E RESPONSABILITÀ

Il *titolare del trattamento dei dati* nella persona del legale rappresentate ha l'obbligo di garantire nei confronti degli interessati il rispetto dei requisiti di protezione dei dati personali.

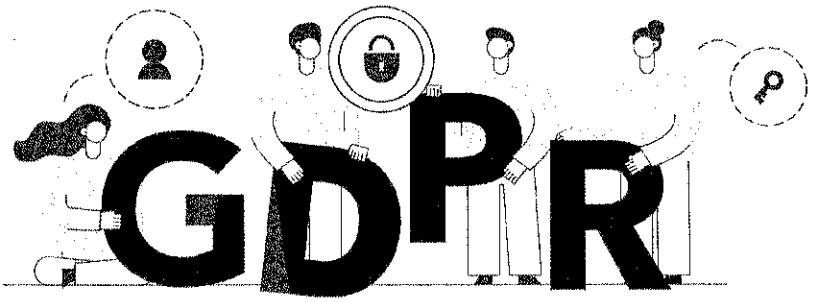
I collaboratori che si occupano dell'elaborazione dei dati personali devono sapere che le violazioni delle norme sulla tutela della privacy vengono perseguite anche penalmente e possono dare luogo a richieste di risarcimento.

Le trasgressioni per le quali possono essere considerati responsabili i singoli collaboratori comportano generalmente le sanzioni previste dal diritto del lavoro, secondo la norma nazionale corrispondente.

NIGRO IMPIANTI SRL

# VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

*Ai sensi del Regolamento (UE)2016/679*




**Titolare del Trattamento:**

## Nigro Impianti S.r.l. con unico socio

| FIGURE | |
|---|---|
| Redatto dal Titolare del Trattamento **Nigro Impianti S.r.l. con unico socio** in collaborazione con i **Responsabili Esterni al Trattamento** | |
| Approvato dal Rappresentante Legale<br>**Antonio Nigro** *(firma)* NIGRO IMPIANTI SRL Via Pacciarella, 31 70022 ALTAMURA (BA) P.Iva: 07337360726 | |
| **Sede** | sede legale: Via Pacciarella - Contrada Bencivenga, 31, 70022, Altamura, (BA) |
| **Data creazione** | 29/07/2015 |
| **Revisione** | 03/11/2023 |
| **Info** | P.IVA: 07337360726<br>Telefono: 080 9140406<br>Email: info@nigroantonioimpiantisrl.it<br>PEC: nigroantonioimpiantisrl@pec.it |

**N.B.**: Con il termine **"Azienda"** si intende il Titolare del Trattamento la cui ragione sociale e dati anagrafici aziendali sono indicati in questa pagina.

NIGRO IMPIANTI SRL

# Sommario

NIGRO IMPIANTI SRL

# 1 PREMESSA

Il presente documento ha l'obiettivo di descrivere i risultati della **DPIA** in riferimento al trattamento dei dati effettuato dall' **AZIENDA.**

L'**obiettivo** è quello di garantire e dimostrare che il trattamento dei dati personali avviene in modo *lecito, corretto e trasparente* al fine di promuovere, attraverso la realizzazione di una gestione interna ben strutturata, la cultura della privacy e della sicurezza dei dati personali.

## 1.1 VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

La **DPIA**, acronimo di *Data Protection Impact Assessment*, è una valutazione d'impatto sulla protezione dei dati, eseguita dal titolare del trattamento e finalizzata a valutare, per le attività di trattamento svolte, quali sono i rischi per i diritti e le libertà degli interessati e in che misura essi si presentano.

In linea con l'approccio basato sul rischio adottato dal regolamento generale sulla protezione dei dati, non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento; **è necessario realizzare una valutazione d'impatto sulla protezione dei dati** soltanto quando la tipologia di trattamento ***"può presentare un rischio elevato per i diritti e le libertà delle persone fisiche"*** **(articolo 35** del Regolamento 2016/679).

## 1.2 OBBLIGO DPIA

Ai sensi *dell'articolo 35, paragrafo 3 del Regolamento 2016/679* è obbligatorio effettuare la valutazione d'impatto nei casi in cui un trattamento può presentare rischi elevati, ossia quando:

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, (dati relativi allo stato di salute) o di dati relativi a condanne penali e a reati di cui all'articolo 10;
c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

## 1.3 CRITERI DA CONSIDERARE PER OBBLIGO DPIA

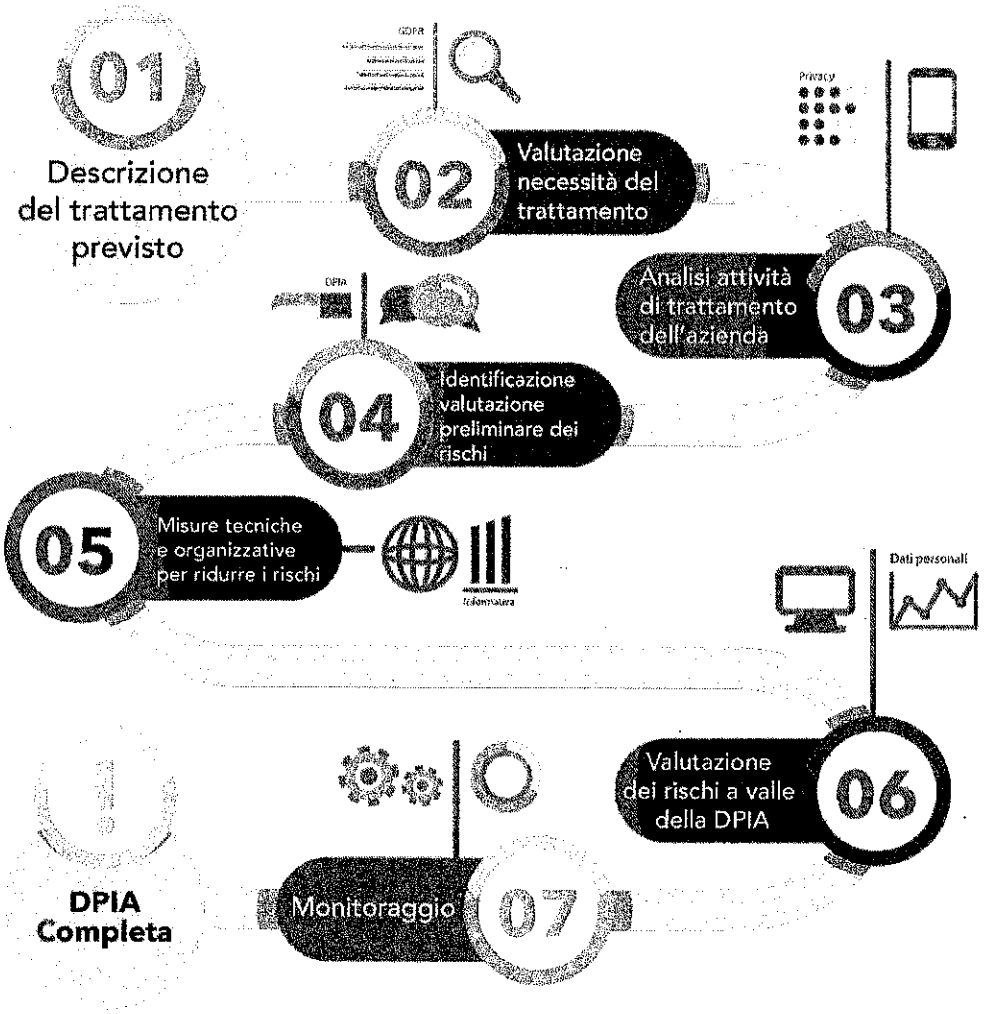
Al fine di valutare se il rischio possa considerarsi elevato, il Gruppo di Lavoro Art. 29, nelle linee guida in materia di valutazione d'impatto, individua 9 criteri ritenendo che maggiore è il numero di criteri soddisfatti più è probabile che sia presente un rischio elevato per i diritti e le libertà degli interessati che rende necessaria la valutazione d'impatto sulla protezione dati.

I **criteri** sono i seguenti:

1) *Valutazione o assegnazione di un punteggio*
2) *Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente*
3) *Monitoraggio sistematico*
4) *Dati sensibili o aventi carattere altamente personale*
5) *Trattamento di dati su larga scala*
6) *Creazione di corrispondenze o combinazione di insieme di dati*
7) *Dati relativi ad interessati vulnerabili*
8) *Uso innovativo o applica zione di nuove soluzioni tecnologiche*
9) *Trattamento che impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto*

Nel caso specifico, per la quantità e la natura dei dati trattati e per le diverse tipologie del loro trattamento, sono presenti rischi elevati per i diritti e le libertà delle persone fisiche, pertanto la DPIA viene effettuata al fine di dimostrarne la responsabilizzazione e la trasparenza del titolare del trattamento per limitarne ulteriormente le possibilità che detti rischi si concretizzino.

## 1.4 FASI PER LA CONDUZIONE DI UNA VALUTAZIONE DI IMPATTO SUI DATI PERSONALI DPIA (Data Protection Impact Assessment)



NIGRO IMPIANTI SRL

## 2 DESCRIZIONE DEL TRATTAMENTO PREVISTO

L'**AZIENDA** raccoglie dati relativi alle seguenti categorie di soggetti:

- ✓ dipendenti, collaboratori;
- ✓ clienti e potenziali clienti;
- ✓ imprese fornitrici
- ✓ imprese collaboratrici (RTI, SUB-APPALTO, AVVALIMENTO)

La **tipologia di dati** trattati rispetto alle suddette categorie può essere la seguente:

- dati anagrafici;
- dati di contatto;
- dati giudiziari;
- dati biometrici;
- dati relativi alla salute;
- dati bancari;
- dati di lavoro.

La base giuridica del trattamento di tali dati da parte dell'**AZIENDA** è rappresentata dall'adempimento degli obblighi contrattuali e precontrattuali, per l'adempimento degli obblighi di legge cui la stessa è tenuta e per finalità amministrativo-contabili.

I dati personali, oltre che trattati dal personale interno all'**AZIENDA** sono comunicati a destinatari nominati *ai sensi dell'art. 28 del GDPR*, che li trattano in qualità di ***Responsabili esterni del trattamento***, al fine di ottemperare agli obblighi di legge, a contratti o a finalità connesse. In particolare i dati possono essere comunicati a destinatari appartenenti alle seguenti categorie:

- Società Partners;
- Studi professionali o Società per rapporti di assistenza e consulenza;
- Istituti di Credito;
- Compagnie Assicurative;
- Enti previdenziali e assistenziali.

Con ciascun **Responsabile esterno del trattamento** è stato stipulato un contratto che espone tutti gli aspetti previsti *dall'art. 28 del GDPR* ossia la durata, l'ambito, la finalità, le istruzioni di trattamento documentate, l'autorizzazione preventiva qualora si ricorra a sub-responsabili.

I dati vengono raccolti in forma cartacea e/o elettronica a seconda delle esigenze di lavoro.

I dati acquisiti in **forma cartacea** sono custoditi in armadi e/o schedari chiusi a chiave all'interno delle stanze dei relativi Responsabili/Incaricati i quali provvedono alla scansione degli stessi onde prevenire la distruzione totale accidentale. I dati acquisiti in **forma elettronica**, ossia trattati mediante personal computers, fissi e/o portatili, i quali sono protetti da passwords richieste all'atto di accensione del terminale.

Il trattamento dei dati personali effettuati mediante l'utilizzo di nuove tecnologie (es. videosorveglianza e geolocalizzazione anche mediante SIM aziendali) presenta un rischio elevato per i diritti e le libertà delle persone pertanto il Regolamento impone l'adozione di misure di sicurezza idonee al fine di limitarne i rischi, già previste nel D. Lgs. 196/2003, ma rese ancor più precise e soggette a sanzioni.

Nel caso specifico l'**AZIENDA possiede** sistemi di videosorveglianza, geolocalizzazione e SIM aziendali.

I dati sono trasferiti a soggetti terzi previo consenso scritto da parte dell'interessato. Il consenso degli interessati deve essere libero, specifico, informato ed inequivocabile, non essendo ammesso il consenso tacito o presunto.

L' **AZIENDA** non trasferisce dati al di fuori dell'**Unione Europea**.

## 3 VALUTAZIONE DI NECESSITÀ DEL TRATTAMENTO IN RELAZIONE ALLE FINALITÀ

Le **operazioni di trattamento dei dati personali** effettuate dall' **AZIENDA** avvengono secondo i *principi di liceità, correttezza e trasparenza*.

Il trattamento è **lecito** in quanto trova fondamento in una base giuridica che, fermo restando in ogni caso l'obbligo di informativa a carico del Titolare del trattamento, prevede il **consenso dell'interessato** ed *è finalizzato all'adempimento degli obblighi contrattuali o precontrattuali.*

Il trattamento è **corretto** in quanto non lede la libertà, la dignità e diritti dell'interessato che non potrà ad esempio essere forzato a conferire i propri dati con artifici di vario genere. Strettamente legato al principio di correttezza vi è quello di **trasparenza**, in base al quale le informazioni e le comunicazioni relative al trattamento di dati personali sono facilmente accessibili e comprensibili mediante un linguaggio semplice e chiaro.

Nello specifico la raccolta dei dati è limitata a quelli necessari per l'esecuzione dei contratti commerciali e di lavoro ed il loro trattamento è altresì finalizzato ad esso.

## 4 ELENCO DELLE ATTIVITÀ SOTTOPOSTE ALLA VALUTAZIONE D'IMPATTO

Di seguito, viene riportata l'analisi di tutte le attività di trattamento dell'**AZIENDA** per cui si è resa necessaria la **Valutazione di Impatto sulla Protezione dei Dati (DPIA)**, nonché le **Misure di Sicurezza adottate,** al fine di garantire la protezione dei dati personali, dimostrando la conformità al Regolamento 2016/679 tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Nell'**identificare i trattamenti** si è provveduto a censire, per le categorie di soggetti indicate nel capitolo 2, tutte le attività di trattamento di dati personali specificandone:

- Il personale coinvolto:
  - Persone autorizzate;
  - Responsabili esterni
- Il processo di trattamento
  - Descrizione;
  - Base giuridica del trattamento;
  - Finalità del trattamento;
  - Tipo di dati trattati;
  - Categorie di destinatari
  - Profilazione;
  - Consenso minori;
  - Geolocalizzazione;
  - Sim aziendali;
  - Termine e cancellazione dati;
  - Trasferimento dati (Paesi extraeuropei);
  - Autorizzazione del garante;
- La modalità di elaborazione dei dati;
  - Strutture informatiche di archiviazione;
  - Strutture di archiviazione cartacea;
  - Strutture informatiche i backup.

NIGRO IMPIANTI SRL

## 4.1 DIPENDENTI, COLLABORATORI ED EVENTUALI FAMILIARI A CARICO

| PERSONALE COINVOLTO | |
|---|---|
| **Persone Autorizzate** | **Area Amministrativa e Area tecnica:** VEDI ORGANIGRAMMA PRIVACY |
| **Responsabili Esterni** | Consulente del lavoro; Commercialista; Consulenti Legali; |
| **Titolare autonomo del trattamento** | Medico Competente |
| **PROCESSO DI TRATTAMENTO** | |
| **Descrizione** | Si trattano i dati personali comunicati per le finalità della gestione del rapporto di lavoro, delle attività formative, di valutazione del personale e dei pagamenti. |
| **Base giuridica per il trattamento dei dati comuni (art. 6 GDPR)** | Consenso; Contratto di lavoro; Legge. |
| **Base giuridica per il trattamento dei dati particolari (art. 9 GDPR)** | Consenso; Contratto di lavoro; Legge. |
| **Finalità del trattamento** | Trattamento giuridico ed economico del personale;<br>Reclutamento, selezione, valutazione del personale;<br>Formazione Professionale<br>Gestione del Personale |
| **Tipo di dati trattati** | dati anagrafici; dati di contatto; dati relativi alla salute; dati bancari; dati biometrici; dati di lavoro; dati giudiziari. |
| **Categorie di destinatari** | Enti previdenziali ed assistenziali; Banche e istituti di credito; Responsabili esterni; Persone autorizzate; Consulenti e liberi professionisti anche in forma associata; Imprese collaboratrici del Titolare del Trattamento. |
| **Profilazione** | SI |
| **Consenso Minori** | NO |
| **Geolocalizzazione** | SI |
| **SIM AZIENDALI** | SI |
| **Termine e cancellazione dati** | I dati saranno trattati per il tempo necessario ad adempiere alle finalità previste nei Contratti di assunzione per lo svolgimento del rapporto contrattuale in essere e per i successivi dieci anni dalla data di acquisizione degli stessi |
| **Trasferimento dati (Paesi Terzi)** | NO |
| **Autorizzazione del Garante** | NON PRESENTE |
| **MODALITA' DI ELABORAZIONE DEI DATI:** | |
| **Strumenti** | Elettronici e cartacei |
| **Strutture informatiche di archiviazione** | |
| **Tipologia** | Personal Computer – Supporti rimovibili – Cellulare - Tablet |
| **Strutture di archiviazione cartacea** | |
| **Tipologia** | Armadietti con serratura |
| **Strutture informatiche di backup** | |
| **Tipologia** | supporti rimovibili ad uso esclusivo del backup |
| **Frequenza Backup** | 7 giorni |
| **Tempo di storicizzazione** | 30 giorni |

## 4.2 CLIENTI E POTENZIALI CLIENTI

| PERSONALE COINVOLTO | |
|---|---|
| **Persone Autorizzate** | **Area Amministrativa**, **Area Tecnica** e **Area Marketing** VEDI ORGANIGRAMMA PRIVACY |
| **Responsabili Esterni** | Commercialista; Consulenti Legali. |
| **PROCESSO DI TRATTAMENTO** | |
| **Descrizione** | Trattamento dei dati personali relativo al rapporto con i clienti |
| **Base giuridica per il trattamento dei dati comuni (art. 6 GDPR)** | Consenso; Contratto di lavoro; Legge. |
| **Base giuridica per il trattamento dei dati particolari (art. 9 GDPR)** | Consenso; Contratto di lavoro; Legge. |
| **Finalità del trattamento** | Erogazione del servizio e/o prodotto;<br>Adempimento di obblighi di legge connessi a rapporti commerciali, nonché obblighi fiscali o contabili (contratti e fatture);<br>Gestione della clientela;<br>Gestione contenziosi. |
| **Tipo di dati trattati** | dati anagrafici; dati di contatto; dati bancari; dati biometrici; |
| **Categorie di destinatari** | Banche e istituti di credito; Responsabili esterni; Persone autorizzate; Consulenti e liberi professionisti anche in forma associata. |
| **Profilazione** | SI |
| **Consenso Minori** | NO |
| **Termine e cancellazione dati** | I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto commerciale in essere e per i successivi 10 anni dalla data di acquisizione degli stessi |
| **Trasferimento dati (Paesi Terzi)** | NO |
| **Autorizzazione del Garante** | NON PRESENTE |
| **MODALITA' DI ELABORAZIONE DEI DATI:** | |
| **Strumenti** | Elettronici e cartacei |
| **Strutture informatiche di archiviazione** | |
| **Tipologia** | Personal Computer – Supporti rimovibili – Cellulare - Tablet |
| **Strutture di archiviazione cartacea** | |
| **Tipologia** | Armadietti con serratura |
| **Strutture informatiche di backup** | |
| **Tipologia** | supporti rimovibili ad uso esclusivo del backup |
| **Frequenza Backup** | 7 giorni |
| **Tempo di storicizzazione** | 30 giorni |

NIGRO IMPIANTI SRL

## 4.3 FORNITORI

| PERSONALE COINVOLTO | |
|---|---|
| **Persone Autorizzate** | **Area Amministrativa, Area Tecnica** e **Area Marketing**: VEDI ORGANIGRAMMA PRIVACY |
| **Responsabili Esterni** | Commercialista; Consulenti Legali. |
| **PROCESSO DI TRATTAMENTO** | |
| **Descrizione** | Gestione contratti di fornitura |
| **Base giuridica per il trattamento dei dati comuni (art. 6 GDPR)** | Consenso; Contratto di lavoro; Legge. |
| **Base giuridica per il trattamento dei dati particolari (art. 9 GDPR)** | Consenso; Contratto di lavoro; Legge. |
| **Finalità del trattamento** | Gestione dei fornitori (contratti, ordini, arrivi, fatture);<br>Elaborazione, stampa e spedizione fatture;<br>Adempimento di obblighi fiscali o contabili;<br>Gestione contenziosi; |
| **Tipo di dati trattati** | dati anagrafici; dati di contatto; dati bancari; dati biometrici. |
| **Categorie di destinatari** | Banche e istituti di credito; Responsabili esterni; Persone autorizzate; Consulenti e liberi professionisti anche in forma associata. |
| **Profilazione** | SI |
| **Consenso Minori** | NON NECESSARIO |
| **Termine e cancellazione dati** | I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto commerciale in essere e per i successivi 10 anni dalla data di acquisizione degli stessi |
| **Trasferimento dati (Paesi Terzi)** | NO |
| **Autorizzazione del Garante** | NON PRESENTE |
| **MODALITA' DI ELABORAZIONE DEI DATI:** | |
| **Strumenti** | Elettronici e cartacei |
| **Strutture Informatiche di archiviazione** | |
| **Tipologia** | Personal Computer – Supporti rimovibili – Cellulare - Tablet |
| **Strutture di archiviazione cartacea** | |
| **Tipologia** | Armadietti con serratura |
| **Strutture Informatiche di backup** | |
| **Tipologia** | supporti rimovibili ad uso esclusivo del backup |
| **Frequenza Backup** | 7 giorni |
| **Tempo di storicizzazione** | 30 giorni |

NIGRO IMPIANTI SRL

## 4.4 IMPRESE COLLABORATRICI: RTI-SUBAPPALTO-AVVALIMENTO

| PERSONALE COINVOLTO | |
|---|---|
| **Persone Autorizzate** | **Area Amministrativa, Area tecnica e Area Marketing**: VEDI ORGANIGRAMMA PRIVACY |
| **Responsabili Esterni** | Commercialista; Consulenti Legali. |
| **PROCESSO DI TRATTAMENTO** | |
| **Descrizione** | Gestione del rapporto di collaborazione con aziende esterne nelle procedure di appalto e di eventuale stipula del contratto in caso di aggiudicazione. |
| **Base giuridica per il trattamento dei dati comuni (art. 6 GDPR)** | Consenso; Contratto di lavoro; Legge. |
| **Base giuridica per il trattamento dei dati particolari (art. 9 GDPR)** | Consenso; Contratto di lavoro; Legge. |
| **Finalità del trattamento** | Adempimento di obblighi di legge e/o contrattuali ai fini della partecipazione della procedura di gara ed all'eventuale stipula del contratto;<br>eventuale gestione del contenzioso;<br>verifica dell'identità e/o idoneità dei soggetti interessati;<br>verifica della regolarità contributiva presso gli enti previdenziali e assistenziali. |
| **Tipo di dati trattati** | dati anagrafici; dati di contatto; dati bancari; dati di lavoro; dati giudiziari; dati biometrici; dati relativi alla salute. |
| **Categorie di destinatari** | Banche e istituti di credito; Responsabili esterni; Persone autorizzate; Stazione appaltante; Consulenti e liberi professionisti anche in forma associata; Imprese di assicurazione. |
| **Profilazione** | SI |
| **Consenso Minori** | NO |
| **Geolocalizzazione** | SI |
| **Termine e cancellazione dati** | I dati saranno trattati per il tempo necessario ad adempiere alle finalità previste dal Contratto, per lo svolgimento del rapporto contrattuale in essere e per i successivi dieci anni dalla data di acquisizione degli stessi |
| **Trasferimento dati (Paesi Terzi)** | NO |
| **Autorizzazione del Garante** | NON PRESENTE |
| **MODALITA' DI ELABORAZIONE DEI DATI:** | |
| **Strumenti** | Elettronici e cartacei |
| | **Strutture informatiche di archiviazione** |
| **Tipologia** | Personal Computer – Supporti rimovibili – Cellulare - Tablet |
| | **Strutture di archiviazione cartacea** |
| **Tipologia** | Armadietti con serratura |
| | **Strutture informatiche di backup** |
| **Tipologia** | supporti rimovibili ad uso esclusivo del backup |
| **Frequenza Backup** | 7 giorni |
| **Tempo di storicizzazione** | 30 giorni |

NIGRO IMPIANTI SRL

# 5 IDENTIFICAZIONE E VALUTAZIONE PRELIMINARE DEI RISCHI

| | DESCRIZIONE DEL RISCHIO | PROBABILITA' DANNO | GRAVITA' DANNO | VALUTAZIONE COMPLESSIVA DEL RISCHIO |
|---|---|---|---|---|
| **Rischio A** | **ACCESSO ILLEGGITTIMO AI DATI**<br>*Le informazioni fornite al titolare del trattamento sono confidenziali e potrebbero arrecare un danno all'interessato qualora circolassero impropriamente.* | BASSA | ALTA | MEDIO |
| **Rischio B** | **MODIFICHE INDESIDERATE DEI DATI**<br>*L'interessato potrebbe subire un danno qualora i suoi dati personali, sebbene utilizzati legittimamente, risultassero non corretti o venissero corrotti durante il trasporto/elaborazione/archiviazione oppure risultassero confuse erroneamente con I dati di un'altra persona.* | BASSA | ALTA | MEDIO |
| **Rischio C** | **PERDITA DEI DATI**<br>*L'interessato ha la legittima aspettativa che i propri dati vengano custoditi in maniera sicura e possano essere recuperati durante l'intero periodo di conservazione. La perdita di dati potrebbe essere causata da:*<br>*- agenti fisici (incendio, allagamento ecc.);*<br>*- eventi naturali (terremoti, eruzioni vulcaniche, ecc.);*<br>*- problemi tecnici (anomalie e malfunzionamenti dei software/hardware);*<br>*- compromissione delle informazioni (intercettazioni, infiltrazioni in posta elettronica, ecc.)* | BASSA | ALTA | MEDIO |

NIGRO IMPIANTI SRL

# 6 MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE PER RIDURRE I RISCHI

Secondo l'**art. 32** del Regolamento le **misure di sicurezza** devono essere approntate "*tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche*".

A tal proposito, dunque l'**AZIENDA.** ha predisposto delle **misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio**, pertanto alla luce dei possibili fattori di rischio connessi al trattamento dei dati per le tre macro-categorie di soggetti interessati – DIPENDENTI, CLIENTI, FORNITORI E IMPRESE COLLABORATRICI – nella tabella seguente vengono descritte le misure atte a garantire la protezione dei dati personali, una descrizione del pericolo associato e il livello di adeguatezza specifico del titolare del trattamento.

NIGRO
IMPIANTI SRL

| | | MISURE DI SICUREZZA |
|---|---|---|
| 1 | **RISCHIO A ACCESSO ILLEGGITTIMO AI DATI** | - Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati;<br>- È applicata una gestione della password degli utenti;<br>- È eseguita la DPIA<br>- È applicata una procedura per la gestione degli accessi<br>- Le password sono costituite da almeno otto caratteri alfanumerici e sono modificate ogni 3 mesi<br>- Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare del trattamento può assicurare la protezione dei dati<br>- Sono definiti ruoli e responsabilità<br>- Sono presenti istruzioni per la custodia e l'uso dei supporti rimovibili<br>- Sono utilizzati software antivirus, anti intrusione e firewall<br>- Vengono registrati e conservati i LOG FILE<br>- Viene eseguita una regolare formazione del personale |
| 2 | **RISCHIO B MODIFICHE INDESIDERATE DEI DATI** | - Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati;<br>- È applicata una gestione della password degli utenti;<br>- È eseguita la DPIA<br>- È applicata una procedura per la gestione degli accessi<br>- Le password sono costituite da almeno otto caratteri alfanumerici e sono modificate ogni 3 mesi<br>- Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare del trattamento può assicurare la protezione dei dati<br>- Sono definiti ruoli e responsabilità<br>- Sono presenti istruzioni per la custodia e l'uso dei supporti rimovibili<br>- Sono utilizzati software antivirus e anti intrusione<br>- Vengono registrati e conservati i LOG FILE<br>- Viene eseguita una regolare formazione del personale<br>- Dispositivi antincendio<br>- Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi |
| 3 | **RISCHIO C PERDITA DEI DATI** | - È eseguita la DPIA<br>- È applicata una procedura per la gestione degli accessi<br>- Le password sono costituite da almeno otto caratteri alfanumerici e sono modificate ogni 3 mesi<br>- Sono effettuati i back up<br>- Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare del trattamento può assicurare la protezione dei dati<br>- Sono definiti ruoli e responsabilità<br>- Sono presenti istruzioni per la custodia e l'uso dei supporti rimovibili<br>- Sono utilizzati software antivirus e anti intrusione<br>- Vengono registrati e conservati i LOG FILE<br>- Viene eseguita opportuna manutenzione delle componenti hardware<br>- Viene eseguita una regolare formazione del personale |

NIGRO IMPIANTI SRL

# 7 VALUTAZIONE DEI RISCHI A VALLE DELLA DPIA

Le valutazioni del rischio sono una parte essenziale della sicurezza dei dati. I rischi da affrontare *riguardano* in particolare quelli derivanti 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, comportando danni alla persona interessata, comprese eventuali discriminazioni, danni alla reputazione, perdita di riservatezza dei dati protetti dal segreto professionale o qualsiasi altro significativo svantaggio economico o sociale.

A tal proposito l'organizzazione deve essere in grado di ripristinare rapidamente la disponibilità e l'accesso ai dati personali dopo una violazione dei dati.

Ciascuna categoria di rischio è valutata in base alla possibilità che esso si verifichi concretamente e può essere:

- *Molto basso*: possibilità quasi nulla che lo scenario possa verificarsi;
- *Basso*: possibilità bassa che lo scenario possa verificarsi;
- *Medio*: possibilità media che lo scenario descritto possa verificarsi;
- *Alto*: lo scenario descritto costituisce un evento quasi certo.

A valle della DPIA, e alla luce delle misure tecniche e organizzative che l'Azienda implementa, l'attività risulta a rischio Molto basso.

| | Descrizione del rischio | VALUTAZIONE COMPLESSIVA DEL RISCHIO |
|---|---|---|
| **Rischio A** | **ACCESSO ILLEGGITTIMO AI DATI**<br>*Le informazioni fornite al titolare del trattamento sono confidenziali e potrebbero arrecare un danno all'interessato qualora circolassero impropriamente.* | MOLTO BASSO |
| **Rischio B** | **MODIFICHE INDESIDERATE DEI DATI**<br>*L'interessato potrebbe subire un danno qualora i suoi dati personali, sebbene utilizzati legittimamente, risultassero non corretti o venissero corrotti durante il trasporto/elaborazione/archiviazione oppure risultassero confuse erroneamente con I dati di un'altra persona.* | MOLTO BASSO |
| **Rischio C** | **PERDITA DEI DATI**<br>*L'interessato ha la legittima aspettativa che i propri dati vengano custoditi in maniera sicura e possano essere recuperati durante l'intero periodo di conservazione. La perdita di dati potrebbe essere causata da:*<br>*- agenti fisici (incendio, allagamento ecc.);*<br>*-eventi naturali (terremoti, eruzioni vulcaniche, ecc.);*<br>*-problemi tecnici (anomalie e malfunzionamenti dei software/hardware);*<br>*-compromissione delle informazioni (intercettazioni, infiltrazioni in posta elettronica, ecc.)* | MOLTO BASSO |

**Nota: Solo se, a valle dell'analisi DPIA, l'attività fosse ricaduta in fascia ALTA, il Titolare del trattamento avrebbe attivato l'iter di consultazione del Garante.**

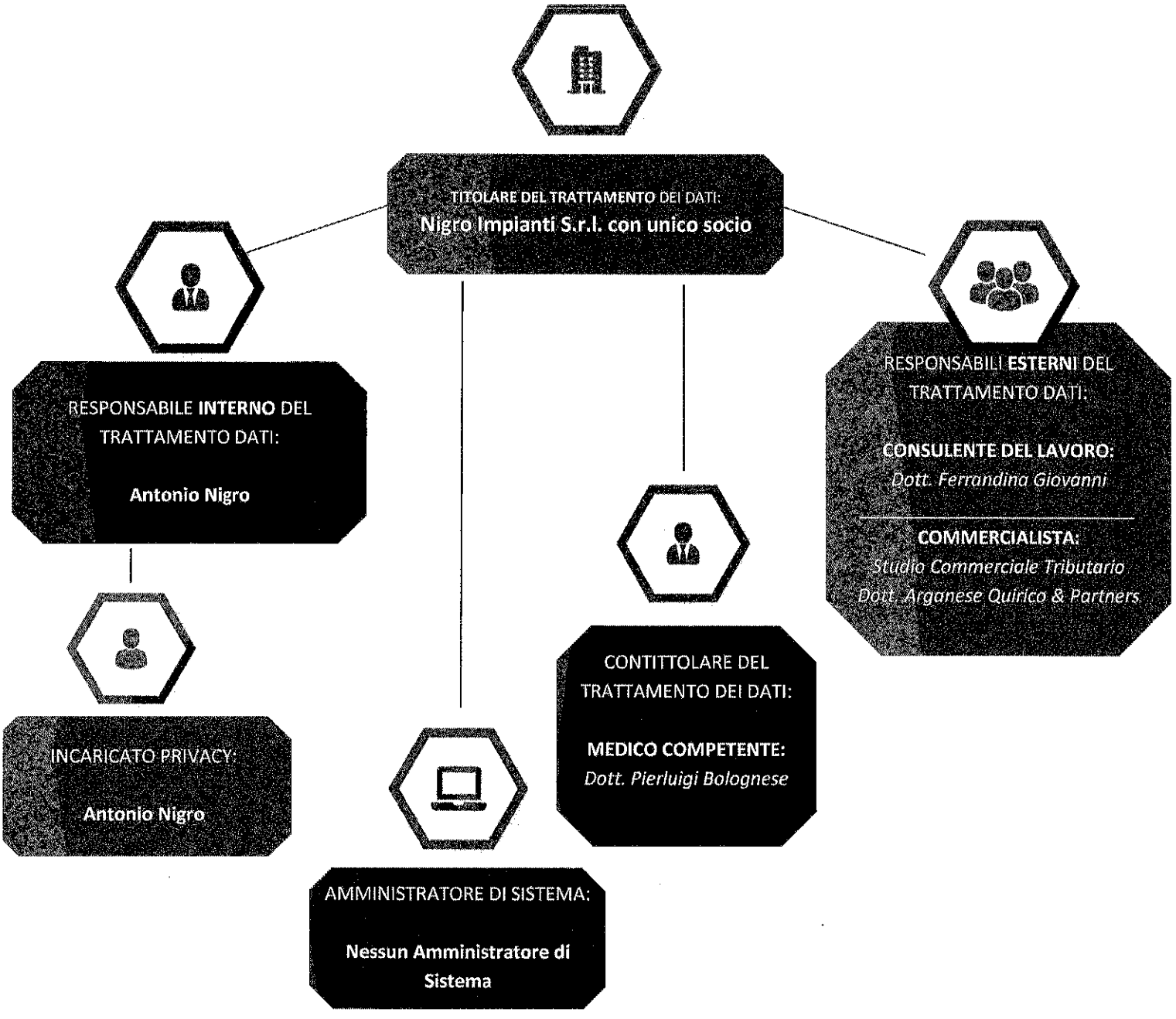
# 8 MONITORAGGIO

L' **AZIENDA** conduce **periodiche valutazioni del rischio** quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento, al fine di garantire un'adeguata protezione dei dati e di dimostrare la concreta attuazione delle misure finalizzate ad assicurare l'applicazione del Regolamento.

NIGRO IMPIANTI SRL

# ORGANIGRAMMA PRIVACY

Revisione n° 2, in data 03/11/2023



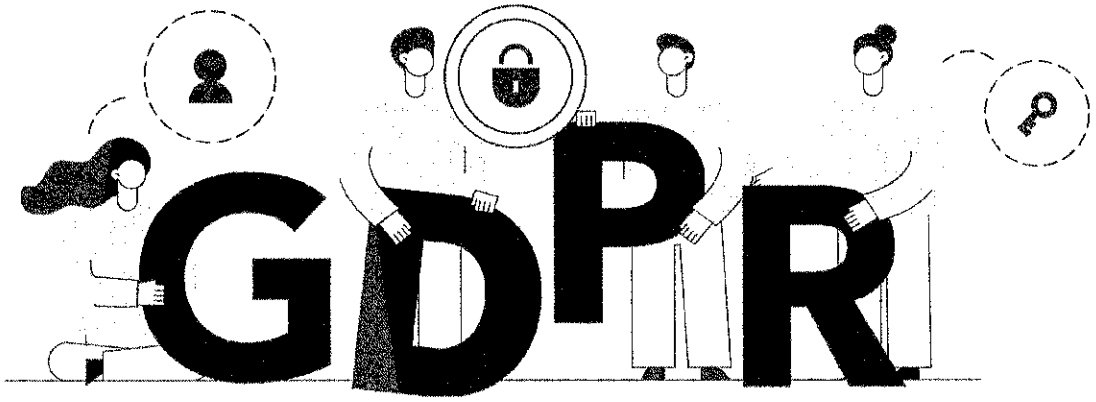

**AUTORIZZATI AL TRATTAMENTO**

Impiegati dell'area **Tecnica** | Impiegati dell'area **Amministrativa** | Impiegati dell'area **Commerciale**

**Nigro Impianti S.r.l. con unico socio**
*Sede Legale*: Via Pacciarella - Contrada Bencivenga, 31, 70022, Altamura, (BA)
C.F. e P.IVA: 07337360726 Tel. 080 9140406
Email: info@nigroantonioimpiantisrl.it – PEC: nigroantonioimpiantisrl@pec.it

# REGISTRO DEL TITOLARE DEL TRATTAMENTO

*Ai sensi del Regolamento (UE)2016/679*




**Titolare del Trattamento:**

## Nigro Impianti S.r.l. con unico socio

| FIGURE | |
|---|---|
| Redatto da Titolare del Trattamento **Nigro Impianti S.r.l. con unico socio** in collaborazione con i **Responsabili Esterni al Trattamento** | |
| Approvato dal Rappresentante Legale<br><br>**Antonio Nigro** | NIGRO IMPIANTI SRL<br>Via Pacciarella, 31<br>70022 ALTAMURA (BA)<br>*(firma)* P.Iva: 07337360726 |
| Sede | sede legale: Via Pacciarella - Contrada Bencivenga, 31, 70022, Altamura, (BA) |
| Info | P.IVA: 07337360726<br>Telefono: 080 9140406<br>Email: info@nigroantonioimpiantisrl.it<br>PEC: nigroantonioimpiantisrl@pec.it |
| Data creazione | 29/07/2015 |
| Revisione e data aggiornamento | Revisione n° 2, in data 03/11/2023 |
| Motivazione | Aggiornamento e verifica privacy. |

# PREMESSA

Il registro del titolare del trattamento si configura come uno strumento che è parte integrante di quel generale sistema di corretta gestione dei dati personali che le aziende o le organizzazioni dovranno creare.

Esso offre una rappresentazione dell'organizzazione sotto il profilo delle attività di trattamento dati ed ha lo scopo di informare, dare consapevolezza e condivisione interna del processo di gestione del dato.

Ai sensi dell'**art. 30** del **GDPR**, il *Registro del Titolare del trattamento* riporta le seguenti informazioni:

- dati di contatto del titolare del trattamento e, dove applicabile, del contitolare del trattamento e del Responsabile della protezione dei dati;
- **finalità del trattamento**, le finalità per le quali sono trattati tali dati;
- categorie di interessati;
- categorie di dati personali;
- categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

NIGRO IMPIANTI SRL

# REGISTRO DEI TRATTAMENTI DEL TITOLARE

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **TITOLARE DEL TRATTAMENTO** | **DENOMINAZIONE:** Nigro Impianti S.r.l. con unico socio | **SEDE LEGALE:** Via Pacciarella - Contrada Bencivenga, 31, 70022, Altamura, (BA) | **C/F - PARTITA IVA:** 07337360726 | **MAIL:** info@nigroantonioimpiantisrl.it | **PEC:** nigroantonioimpiantisrl@pec.it | **TELEFONO:** 080 9140406 | **FAX:** 080 2142585 |
| **RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO)** | | **Non Nominato** | | **CONTITOLARE DEL TRATTAMENTO** | | **Medico Competente** Dott. Pierluigi Bolognese | |
| **RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI** | | **Commercialista** Studio Commerciale Tributario, Dott. Arganese Quirico & Partners | | **RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI** | | **Consulente del lavoro** Dott. Giovanni Ferrandina | |

| Tipologia Di Trattamento | Finalità e Basi Legali del Trattamento | Categorie di interessati | Categorie di Dati Personali | Categorie di Destinatari | Trasferimento Dati Verso Paesi Terzi o Organizzazioni internazionali | Termini Ultimi di Cancellazione Previsti | Misure di Sicurezza Tecniche e Organizzative |
|---|---|---|---|---|---|---|---|
| **Trattamento legato al rapporto contrattuale con dipendenti e collaboratori** | Gestione del rapporto di lavoro o di collaborazione. | Dipendenti e loro familiari, collaboratori | Dati anagrafici; Dati bancari; Dati biometrici; Dati relativi alla salute; Dati di lavoro; | Enti previdenziali ed assistenziali; Banche e istituti di credito; Responsabili esterni; Persone autorizzate; Consulenti e liberi professionisti anche in forma associata; Imprese collaboratrici del Titolare del Trattamento. | NO | 10 anni dalla data di acquisizione dei dati o al termine del rapporto di lavoro o di collaborazione. | Procedure e tecniche organizzative interne a tutela della privacy e per la limitazione dei rischi. Si rimanda alle **Procedure** contenute nel **Manuale GDPR.** |
| **Trattamento legato al rapporto contrattuale con clienti e potenziali clienti** | Gestione della clientela finalizzata alla erogazione del servizio offerto | Clienti e potenziali clienti | Dati anagrafici; Dati bancari; Dati biometrici; | Responsabili interni, Banche e istituti di credito; Responsabili esterni; Persone autorizzate; Consulenti e liberi professionisti anche in forma associata; | NO | 10 anni dalla data di acquisizione dei dati o al termine del rapporto contrattuale | Procedure e tecniche organizzative interne a tutela della privacy e per la limitazione dei rischi. Si rimanda alle **Procedure** contenute nel **Manuale GDPR.** |
| **Trattamento legato al rapporto contrattuale con fornitori** | Gestione degli ordini (contratti ordini e fatture) | Fornitori | Dati anagrafici; Dati bancari; Dati biometrici; | Banche e istituti di credito; Responsabili esterni; Persone autorizzate; Consulenti e liberi professionisti anche in forma associata; | NO | 10 anni dalla data di acquisizione dei dati o al termine del rapporto commerciali. | Procedure e tecniche organizzative interne a tutela della privacy e per la limitazione dei rischi. Si rimanda alle **Procedure** contenute nel **Manuale GDPR.** |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Trattamento legato al rapporto contrattuale con imprese collaboratrici (RTI, subappalto, avvalimento)** | Gestione del rapporto contrattuale con le imprese collaboratrici | Imprese collaboratrici (RTI, subappalto, avvalimento) | Dati anagrafici; Dati bancari; Dati di lavoro; Dati giudiziari; Dati relativi alla salute; Dati biometrici; | Enti previdenziali ed assistenziali; Banche e istituti di credito; Responsabili esterni; Persone autorizzate; Stazione appaltante; Consulenti e liberi professionisti anche in forma associata; Imprese di assicurazione. | NO | 10 anni dalla data di acquisizione dei dati o al termine del rapporto commerciali. | Procedure e tecniche organizzative interne a tutela della privacy e per la limitazione dei rischi. Si rimanda alle **Procedure** contenute nel **Manuale GDPR.** |
| **Trattamento legato al rapporto contrattuale con dipendenti e collaboratori** | Gestione dell'incarico per lo svolgimento dei compiti previsti dal D. Lgs. N. 81/2008 in materia di sorveglianza sanitaria | Lavoratori e collaboratori azienda | Personali quali l'anagrafica (es. nome, cognome, indirizzo, codice fiscale, data assunzione, mansione); Particolari (es. dati anamnestici, dati relativi allo stato di salute, dati biometrici, ecc…) | Enti previdenziali ed assistenziali; Persone autorizzate; | NO | 10 anni dalla data di acquisizione dei dati o al termine del rapporto di lavoro o di collaborazione. | Procedure e tecniche organizzative interne a tutela della privacy e per la limitazione dei rischi. Si rimanda alle **Procedure** contenute nel **Manuale GDPR.** |

CONFLAVORO
Piccole Medie Imprese

OPNASP
ORGANISMO PARITETICO NAZIONALE SETTORE PRIVATO

# Attestato di Frequenza

si certifica e attesta che

## ANTONIO NIGRO

Nato il 18/04/1973 in ALTAMURA (BA) - NGRNTN73D18A225L

Mansione: Amministratore Settore: 43.21.01 Azienda: Nigro Impianti S.r.l. con unico socio

ha partecipato, superando con esito positivo la verifica finale di apprendimento, per il corso di formazione:

**ADDETTO AL TRATTAMENTO DEI DATI PRIVACY**

**GDPR - General Data Protection Regulation**

2 ore (due)

ai sensi dell'art. 29 del Regolamento Europeo GDPR 679/2016

Soggetto Organizzatore Accreditato CFPT Conflavoro PMI EB00F318

(Centro di Formazione Paritetico Territoriale)

**DI.SA. SRL**
**Via Appia,126- Loc. Castello del Lago - 83030 - Venticano - AV**
**P.Iva 01463390623**

Il corso è stato eseguito in modalità :
Elearning

LMS utilizzata
www.fadcertificata.it

Data fine corso
28/11/2023

Valido fino al: 28/11/2028

DI SA
Servizi alle imprese

Conflavoro PMI
Confederazione Nazionale Piccole e Medie Imprese
Segretario Generale Nazionale

OPNASP
Organismo Paritetico Nazionale Settore Privato
APPROVATO
www.opnasp.it

Direttore CFPT
Nadia Di Stasio

N° PROTOCOLLO EB00F318/2023/0043

Verifica l'autenticità dell'attestato sul sito www.unasf.conflavoro.it o scansiona il QR Code

Soggetto Formatore Conflavoro PMI – Confederazione Nazionale Piccole e Medie Imprese in collaborazione con l'Organismo Paritetico OPNASP

**Nigro Impianti S.r.l. con unico socio**
Via Pacciarella - Contrada Bencivenga, 31 - 70022 Altamura (BA)
Tel: 080 9140406 / Fax: 080 2142585
Email: info@nigroantonioimpiantisrl.it - PEC: nigroantonioimpiantisrl@pec.it
P.IVA: 07337360726



# Procedura per la gestione delle richieste di esercizio dei diritti degli interessati
## Artt. 15 - 22 del Regolamento UE 2016/679 (GDPR)

***



***

## Premessa

### Scopo
Scopo della presente procedura è definire i compiti, le responsabilità e le modalità operative da adottare qualora venga presentata al Titolare del trattamento una richiesta per l'esercizio dei diritti da parte degli interessati in ordine al trattamento dei dati personali effettuato da o per conto della Nigro Impianti S.r.l. con socio unico.
La presente procedura è portata a conoscenza di tutti i Dirigenti, Dipendenti e Collaboratori della società.

### Riferimenti normativi
- Decreto Legislativo n. 196/2003 e ss.mm.ii. (c.d. Codice privacy).
- Regolamento (UE) 2016/679 (GDPR) e ss.mm.ii..

**Nigro Impianti S.r.l. con unico socio**
Via Pacciarella - Contrada Bencivenga, 31 - 70022 Altamura (BA)
Tel: 080 9140406 / Fax: 080 2142585
Email: info@nigroantonioimpiantisrl.it - PEC: nigroantonioimpiantisrl@pec.it
P.IVA: 07337360726

NIGRO IMPIANTI SRL

## Acronimi e definizioni utilizzate

| | |
|---|---|
| **GDPR:** | Regolamento UE 2016/679 (General Data Protection Regulation) |
| **Codice D.Lgs. 196/2003:** | "Codice in materia di protezione dei dati personali" come modificato dal D.Lgs. 101/2018 |
| **Garante:** | Garante per la protezione dei dati personali |
| **Titolare del trattamento:** | Nigro Impianti S.r.l. con socio unico |
| **Responsabile esterno del trattamento:** | soggetto esterno che tratta dati personali per conto del Titolare (art. 28 GDPR) |
| **Referente/Autorizzato:** | soggetto interno nominato per la gestione delle richieste per l'esercizio di diritti in materia di protezione dei dati personali |
| **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 |
| **Interessato:** | la persona fisica identificata o identificabile cui si riferiscono i dati personali |

## 1. I Diritti degli interessati

Gli interessati possono esercitare, ai sensi degli artt. 15 e ss. del GDPR con riferimento ai propri dati personali detenuti dalla Nigro Impianti S.r.l. con socio unico, i seguenti diritti:

a) **di accesso (art.15)**: ottenere dal Titolare del trattamento, in qualsiasi momento, la conferma o meno dell'esistenza di un trattamento di dati personali che lo riguardano, senza necessità di motivare la richiesta. In caso positivo l'interessato ha altresì diritto di ottenere l'accesso ai dati e ottenerne una copia e, inoltre, di essere informato su finalità del trattamento, categorie di dati, destinatari, il periodo per il quale i dati saranno archiviati
b) **di rettifica o integrazione (art.16)**: ottenere che i dati inesatti o incompleti siano modificati o completati
c) **alla cancellazione (art.17):** far cancellare tutti i dati, link, copia e riproduzione (se diffusi pubblicamente) in presenza di determinati presupposti
d) **alla limitazione (art. 18)**: a determinate condizioni, contrassegnare i dati al fine di limitare il loro trattamento (ad esempio in caso di contestazione dell'esattezza dei dati stessi)
e) **alla portabilità dei dati (art. 20):** diritto di ricevere i dati trattati con strumenti automatizzati in un formato digitale comunemente utilizzato e leggibile e diritto di richiedere di trasmettere tali dati a un altro titolare (ove tecnicamente fattibile)
f) **di opposizione (art.21)**: opporsi, a determinate condizioni, al trattamento dei dati

g) **di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato (art. 22):** opporsi al trattamento, quando le decisioni che lo riguardano e che producono effetti giuridici o incidono significativamente sulla sua persona, vengono assunte unicamente in base ad un processo automatizzato, senza il coinvolgimento di un essere umano

I diritti di cui agli artt. da 15 a 22 del GDPR riferiti ai dati personali concernenti persone decedute - ai sensi dell'art. 2-*terdecies*, comma 1, del D.Lgs. n. 196/2003 – "*possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione*".

## 2. Ruoli e responsabilità

La procedura si applica a tutti i dipendenti e collaboratori della Nigro Impianti S.r.l. con socio unico, nonché ai Responsabili del trattamento, nominati ai sensi dell'art. 28 del GDPR, per gli aspetti che riguardano la gestione delle richieste per l'esercizio dei diritti riconosciuti all'interessato.
Il rispetto della presente procedura è obbligatorio ed è richiesto il sollecito e attivo coinvolgimento dei soggetti sopra richiamati. Gli stessi sono tenuti, di conseguenza, a fornire al Titolare del trattamento la massima collaborazione per il rispetto di quanto previsto dalla normativa sopra richiamata.

## 3. Fasi della procedura

### Presentazione e ricezione della richiesta

La richiesta può pervenire direttamente al Titolare ovvero essere intercettata dai soggetti terzi che, operando in qualità di Responsabili del trattamento, si trovino in contatto diretto con gli interessati stessi.
Le richieste possono essere esercitate utilizzando l'apposito modulo "*Esercizio di diritti in materia di protezione dei dati personali*" di cui all'all. A, da inoltrare tramite mail all'indirizzo indicato. Alla richiesta dovrà essere allegata – a pena di irricevibilità - copia del documento d'identità del richiedente (a meno che l'istanza non sia con la firma digitale del richiedente).
La richiesta dovrà essere trasmessa al seguente indirizzo e-mail: *info@nigroantonioimpiantisrl.it*
La richiesta è sempre oggetto di protocollazione, al fine di attribuirvi la data di ricezione utile al calcolo dei termini di cui al paragrafo successivo
Requisito soggettivo per l'esercizio dei diritti di cui trattasi è che le richieste si riferiscano a informazioni relative a "persone fisiche" detenute dalla Nigro Impianti S.r.l. con socio unico.
L'interessato che esercita un diritto deve essere identificato, ai fini della più corretta istruttoria delle richieste.
Per i diritti concernenti le persone decedute è necessario verificare la legittimazione del richiedente. Secondo quanto affermato dalla giurisprudenza e dal Garante, la legittimazione può essere esercitata non solo dagli eredi, ma anche da chiunque vi abbia un interesse proprio ovvero agisca a tutela dell'interessato o per ragioni familiari meritevoli di protezione.

### Valutazione della richiesta

Il Titolare del trattamento, effettua la valutazione della richiesta presentata dall'interessato allo scopo di appurare la fondatezza dell'istanza e porre in essere le azioni necessarie per evadere la richiesta. Qualora dalla valutazione dell'istanza emergano ragionevoli dubbi circa l'identità della persona fisica che presenta la richiesta, il Titolare provvederà ad informare l'interessato.

**Nigro Impianti S.r.l. con unico socio**
Via Pacciarella - Contrada Bencivenga, 31 - 70022 Altamura (BA)
Tel: 080 9140406 / Fax: 080 2142585
Email: info@nigroantonioimpiantisrl.it - PEC: nigroantonioimpiantisrl@pec.it
P.IVA: 07337360726

NIGRO IMPIANTI SRL

### Reperimento dei dati ed esecuzione delle operazioni richieste dall'interessato

Se l'istanza è ritenuta fondata il Titolare provvederà ad identificare la struttura organizzativa coinvolta, prevedendo il necessario coinvolgimento dei Soggetti Designati o dei Responsabili del trattamento che detengono i dati oggetto dell'istanza.
Una volta verificata l'esistenza dei dati rappresentati nell'istanza, si procederà a svolgere le operazioni richieste ai sensi degli artt. da 15 a 22 del GDPR (ad es. rettifica, integrazione, cancellazione, ecc.).
Nel caso in cui norme di legge o di regolamento non consentano di ottemperare a quanto contenuto nell'istanza, si procederà a predisporre le opportune motivazioni e a fornire riscontro all'interessato.

### Riscontro all'interessato

Ai sensi dell'art. 12, paragrafo 3, del GDPR, il Titolare del trattamento fornisce all'interessato le informazioni relative all'azione intrapresa riguardo alla richiesta di esercizio dei diritti allo stesso riconosciuti, senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta, anche qualora la risposta abbia esito negativo.
Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste ricevute. In caso di estensione del termine di risposta, il Titolare del trattamento è tenuto a informare l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta.
In caso di inottemperanza alla richiesta dell'interessato, il Titolare del trattamento informa l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale.
La risposta deve essere formulata in forma concisa, trasparente e intellegibile e redatta con linguaggio semplice e chiaro.
La modalità di risposta deve tenere in considerazione il canale indicato dall'interessato nella richiesta.
Nel caso venga richiesto l'esercizio del diritto di portabilità di cui all'art. 20 del GDPR, il riscontro dovrà avvenire mediante allegazione in formato elettronico dei dati secondo lo standard esplicato nelle "Linee-guida sul diritto alla portabilità dei dati" - WP242, adottate dal Gruppo di lavoro Art. 29, disponibili in www.garanteprivacy.it/regolamentoue/portabilita.
Ai sensi dell'art. 12, paragrafo 2, del GDPR, nel caso di trattamento dei dati effettuato per una finalità che non richieda, o non richieda più, l'identificazione dell'interessato, il Titolare non può rifiutare di soddisfare la richiesta dell'interessato al fine dell'esercizio dei suoi diritti, salvo che il Titolare dimostri che non è in grado di identificare l'interessato. In tale ultimo caso i diritti potranno essere esercitati solo quando l'interessato fornisce ulteriori informazioni che ne consentano l'identificazione.

### Costi per la gestione delle richieste

Le operazioni riguardanti la gestione delle richieste volte all'esercizio dei diritti riconosciuti dal GDPR vengono effettuate senza costi per l'interessato.
Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il Titolare del trattamento può addebitare un contributo spese ragionevole, tenendo conto dei costi amministrativi sostenuti per gestire la richiesta, oppure rifiutarsi di soddisfare la richiesta, come previsto dall'art. 12, paragrafo 5, del GDPR. Incombe al Titolare del trattamento l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

### Archiviazione della documentazione

La documentazione relativa alle richieste di esercizio dei diritti da parte degli interessati viene conservata dal Titolare del trattamento, per dieci anni dalla protocollazione della richiesta.

**Nigro Impianti S.r.l. con unico socio**
Via Pacciarella - Contrada Bencivenga, 31 - 70022 Altamura (BA)
Tel: 080 9140406 / Fax: 080 2142585
Email: info@nigroantonioimpiantisrl.it - PEC: nigroantonioimpiantisrl@pec.it
P.IVA: 07337360726

### Notifica in caso di rettifica, cancellazione o limitazione del trattamento

Ai sensi dell'art. 19 del GDPR, il Titolare del trattamento ha la responsabilità di comunicare a ciascuno dei destinatari cui sono stati trasmessi i dati personali, le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma degli articoli 16, 17, paragrafo 1, e 18 del GDPR, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato.
La comunicazione ai soggetti di cui sopra è effettuata dal Titolare del trattamento, entro il termine di un mese dal momento dell'intervento di rettifica e/o cancellazione effettuato sui dati o di limitazione del trattamento, tenendone traccia nel Registro delle richieste di esercizio dei diritti degli interessati.
Qualora il soggetto interessato ne abbia fatto richiesta, il Titolare del trattamento fornisce evidenza dei soggetti cui sono stati trasmessi i dati personali che lo riguardano.

### 4. Registro delle richieste di esercizio dei diritti degli interessati

Il Titolare documenta le istanze volte all'esercizio dei diritti dell'interessato mediante la predisposizione di un Registro interno aggiornato.
Il Registro delle richieste di esercizio dei diritti degli interessati dovrà contenere le informazioni di seguito riportate:
- n. progressivo
- data di ricezione dell'istanza
- numero di protocollo assegnato
- nominativo del richiedente
- nominativo dell'interessato (se diverso dal richiedente)
- descrizione della richiesta
- strutture organizzative o banche dati coinvolte
- azione intrapresa riguardo alla richiesta
- riferimenti della nota di riscontro all'interessato (data e protocollo)
- note e commenti.

**Nigro Impianti S.r.l. con unico socio**
Via Pacciarella - Contrada Bencivenga, 31 - 70022 Altamura (BA)
Tel: 080 9140406 / Fax: 080 2142585
Email: info@nigroantonioimpiantisrl.it - PEC: nigroantonioimpiantisrl@pec.it
P.IVA: 07337360726

**ALLEGATO A**

Alla cortese attenzione della
*Nigro Impianti S.r.l.*
*In persona del legale rappresentante p.t.*

**ESERCIZIO DI DIRITTI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI**
*(artt. 15-22 del Regolamento (UE) 2016/679)*

***

Il/La sottoscritto/a..... nato/a a..... il....., esercita con la presente richiesta i seguenti diritti di cui agli artt. 15-22 del Regolamento (UE) 2016/679:

**1. Accesso ai dati personali** *(art. 15 del Regolamento (UE) 2016/679)*
Il sottoscritto *(barrare solo le caselle che interessano)*:

chiede conferma che sia o meno in corso un trattamento di dati personali che lo riguardano;
in caso di conferma, chiede di ottenere l'accesso a tali dati, una copia degli stessi, e tutte le informazioni previste alle lettere da a) a h) dell'art. 15, paragrafo 1, del Regolamento (UE) 2016/679, e in particolare;

- le finalità del trattamento;
- le categorie di dati personali trattate;
- i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
- il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'origine dei dati (ovvero il soggetto o la specifica fonte dalla quale essi sono stati acquisiti);
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e le informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

**Nigro Impianti S.r.l. con unico socio**

Via Pacciarella - Contrada Bencivenga, 31 - 70022 Altamura (BA)

Tel: 080 9140406 / Fax: 080 2142585

Email: info@nigroantonioimpiantisrl.it - PEC: nigroantonioimpiantisrl@pec.it

P.IVA: 07337360726

## 2. Richiesta di intervento sui dati *(artt. 16-18 del Regolamento (UE) 2016/679)*

Il sottoscritto chiede di effettuare le seguenti operazioni *(barrare solo le caselle che interessano)*:

rettificazione e/o aggiornamento dei dati (art. 16 del Regolamento (UE) 2016/679);

cancellazione dei dati (art. 17, paragrafo 1, del Regolamento (UE) 2016/679), per i seguenti motivi *(specificare quali)*:

_____

_____

_____

nei casi previsti all'art. 17, paragrafo 2, del Regolamento (UE) 2016/679, l'attestazione che il titolare ha informato altri titolari di trattamento della richiesta dell'interessato di cancellare

link, copie o riproduzioni dei suoi dati personali;

limitazione del trattamento (art. 18) per i seguenti motivi *(barrare le caselle che interessano)*:

contesta l'esattezza dei dati personali;

il trattamento dei dati è illecito;

i dati sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;

l'interessato si è opposto al trattamento dei dati ai sensi dell'art. 21, paragrafo 1, del Regolamento (UE) 2016/679.

La presente richiesta riguarda (indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento):

_____

_____

_____

_____

_____

_____

_____

_____

_____

**Nigro Impianti S.r.l. con unico socio**

Via Pacciarella - Contrada Bencivenga, 31 - 70022 Altamura (BA)

Tel: 080 9140406 / Fax: 080 2142585

Email: info@nigroantonioimpiantisrl.it - PEC: nigroantonioimpiantisrl@pec.it

P.IVA: 07337360726

## 3.Portabilità dei dati[1] *(art. 20 del Regolamento (UE) 2016/679)*

Con riferimento a tutti i dati personali forniti al titolare, il sottoscritto chiede di *(barrare solo le caselle che interessano)*:

ricevere tali dati in un formato strutturato, di uso comune e leggibile da dispositivo automatico;

trasmettere direttamente al seguente diverso titolare del trattamento *(specificare i riferimenti identificativi e di contatto del titolare: .....):*

tutti i dati personali forniti al titolare;

un sottoinsieme di tali dati.

La presente richiesta riguarda (indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento):

_____

_____

_____

_____

_____

_____

_____

_____

_____

[1] Per approfondimenti: Linee-guida sul diritto alla "portabilità dei dati" - WP242, adottate dal Gruppo di lavoro Art. 29, disponibili in www.garanteprivacy.it/regolamentoue/portabilita.

**Nigro Impianti S.r.l. con unico socio**
Via Pacciarella - Contrada Bencivenga, 31 - 70022 Altamura (BA)
Tel: 080 9140406 / Fax: 080 2142585
Email: info@nigroantonioimpiantisrl.it - PEC: nigroantonioimpiantisrl@pec.it
P.IVA: 07337360726

**4. Opposizione al trattamento** *(art. 21, paragrafo 1 del Regolamento (UE) 2016/679)*

Il sottoscritto si oppone al trattamento dei suoi dati personali ai sensi dell'art. 6, paragrafo 1, lettera e) o lettera f), per i seguenti motivi legati alla sua situazione particolare (specificare):

_____
_____
_____
_____
_____
_____

**5. Opposizione al trattamento per fini di marketing diretto** *(art. 21, paragrafo 2 del Regolamento (UE) 2016/679)*

Il sottoscritto si oppone al trattamento dei dati effettuato a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

_____

Il sottoscritto:

Chiede di essere informato, ai sensi dell'art. 12, paragrafo 4 del Regolamento (UE) 2016/679, al più tardi entro un mese dal ricevimento della presente richiesta, degli eventuali motivi che impediscono al titolare di fornire le informazioni o svolgere le operazioni richieste.
Chiede, in particolare, di essere informato della sussistenza di eventuali condizioni che impediscono al titolare di identificarlo come interessato, ai sensi dell'art. 11, paragrafo 2, del Regolamento (UE) 2016/679.

_____

**Nigro Impianti S.r.l. con unico socio**
Via Pacciarella - Contrada Bencivenga, 31 - 70022 Altamura (BA)
Tel: 080 9140406 / Fax: 080 2142585
Email: info@nigroantonioimpiantisrl.it - PEC: nigroantonioimpiantisrl@pec.it
P.IVA: 07337360726

NIGRO
IMPIANTI SRL

**Recapito per la risposta[2]:**

Via/Piazza

Comune Provincia Codice postale

oppure

e-mail/PEC:

**Eventuali precisazioni**

Il sottoscritto precisa (fornire eventuali spiegazioni utili o indicare eventuali documenti allegati):

(Luogo e data)
(Firma)

[2] Allegare copia di un documento di riconoscimento