**Organizzazione**

# Azienda Trasporti Funicolari Malcesine Monte Baldo

C.so Porta Nuova, 96 – 37122 Verona (VR)
Tel. +39 0457400206
Web : www.funiviedelbaldo.it
E-Mail : info@funiviedelbaldo.it

# Codice di autoregolamentazione dei dati personali

| | |
|---|---|
| **Master** | √ |
| **Copia controllata** | √ |
| **Copia non controllata** | × |
| **Numero della copia** | 01 |

| | |
|---|---|
| **Approvazione CDA** | **Approvato con delibera del Consiglio di Amministrazione n. 4/38 del 29.04.2025** |

**Stato delle revisioni**

| Versione | Data | Descrizione | Autore |
|---|---|---|---|
| 00 | *24.10.2024* | Prima emissione | Avv. Riccardo Berti |

## Indice generale della sezione

## DEFINIZIONI

INTERESSATO: la persona fisica identificata o identificabile cui si riferiscono i dati personali. Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo quale il nome e/o il cognome, 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.

DATO PERSONALE: qualsiasi informazione concernente una persona fisica identificata o identificabile (interessato).

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.

TITOLARE DEL TRATTAMENTO: la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi 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 del trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

CONTITOLARI DEL TRATTAMENTO: si definiscono tali due o più titolari del trattamento che determinano congiuntamente le finalità e i mezzi del trattamento.

RESPONSABILE DEL TRATTAMENTO: la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che tratta dati personali per conto del Titolare del trattamento.

DESTINATARIO: la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi 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 in materia di protezione dei dati applicabili secondo le finalità del trattamento.

TERZO: la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati sotto l'autorità diretta del titolare o del responsabile.

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 personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento

professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

PSEUDONIMIZZAZIONE: il trattamento dei dati personali in moto tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive.

ARCHIVIO: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati.

CONSENSO DELL'INTERESSATO: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

VIOLAZIONE DEI DATI PERSONALI (DATA BREACH): la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

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

DATI BIOMETRICI: i dati personali ottenuti da un trattamento tecnico specifico relativo alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

DATI RELATIVI ALLA SALUTE: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la presentazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

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.

NORME VINCOLANTI D'IMPRESA: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune.

AUTORITA' DI CONTROLLO: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'art. 51 del Regolamento UE 2016/679. In Italia è l'autorità di controllo è il Garante per la protezione dei dati personali.

## PARTE GENERALE

### 1.0 Ambito di applicazione

Il Regolamento europeo sulla privacy, Regolamento UE 2016/679 approvato il 14 aprile 2016 dal Parlamento UE (d'ora innanzi per brevità anche denominato "GDPR"), stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati. Il Regolamento, infatti, si è posto come obiettivo quello di proteggere i diritti e le libertà fondamentali delle persone fisiche, in particolare il loro diritto alla protezione dei dati personali (artt. 8 par. 1 e 16 par. 1 della Carta dei diritti fondamentali dell'Unione europea).
Il Regolamento ha, in concreto, introdotto una serie di nuovi adempimenti in capo ai titolari del trattamento ponendo maggiore attenzione in relazione ai diritti degli interessati.
Infatti, in relazione ai diritti degli interessati, si vede un potenziamento dei contenuti obbligatori dell'informativa, vi è ad esempio:

- l'introduzione del diritto ad una cancellazione estesa dei propri dati personali (diritto all'oblio) tuttavia, tale cancellazione non è incondizionata essendo comunque previste limitazioni all'esercizio del diritto per contemperare altre esigenze e interessi legittimi (libertà di espressione, interesse pubblico, finalità archivistiche nel pubblico interesse);
- l'introduzione della possibilità di chiedere la "limitazione" del trattamento - anziché la cancellazione - ad esempio in attesa di definire l'esattezza o obsolescenza di un dato o per continuare ad utilizzare il dato per specifiche finalità, in particolare giudiziarie;
- previsione di una forma di consenso rafforzato qualora vi si ricorra per legittimare il trattamento dei dati personali.

In riferimento agli obblighi introdotti per i titolari del trattamento invece, si richiamano ad esempio i seguenti:

- introduzione del c.d. "approccio basato sul rischio" e, più in generale, del principio di accountability, ovvero di responsabilizzazione dei titolari di trattamento. Ciò si traduce in una serie di disposizioni che tendono a promuovere approcci proattivi, e non reattivi, in un'ottica di prevenzione di possibili problematiche e di riduzione degli oneri considerati puramente burocratici, quali la notifica dei trattamenti. Si ricordano le principali:
  a. applicazione dei principi di privacy by design e privacy by default in via generale;
  b. obbligo per tutti i titolari / responsabili di condurre una valutazione d'impatto prima di procedere ad un nuovo trattamento, seguita eventualmente dalla consultazione dell'Autorità di controllo qualora il titolare non ritenga sufficienti le misure di mitigazione del rischio a lui note o disponibili;
  c. introduzione e disciplina della figura del responsabile della protezione dati (ovvero Data Protection Officer DPO), la cui nomina è obbligatoria per i soggetti pubblici, mentre è facoltativa per i privati ad eccezione di alcuni trattamenti particolarmente a rischio e salva diversa disposizione della legislazione nazionale. Il regolamento fissa i requisiti essenziali in termini di indipendenza, conoscenza e compiti del DPO;
  d. disciplina specifica della contitolarità di trattamento e della ripartizione di responsabilità fra contitolari, e specificazione del vincolo di natura contrattuale che deve sussistere fra titolare e responsabile del trattamento;
  e. eliminazione dell'obbligo di notifica dei trattamenti all'Autorità, sostituita dall'obbligo di tenuta di documentazione sui trattamenti svolti, a disposizione dell'Autorità (registro dei trattamenti);

f. introduzione dell'obbligo generalizzato per tutti i titolari di notifica di eventuali violazioni di dati personali (personal data breach), all'Autorità ed agli interessati, secondo un criterio di rischio più o meno elevato per i diritti dell'interessato stesso;
g. potenziamento del ricorso a codici deontologici (anche settoriali) e introduzione dell'istituto della certificazione dei trattamenti, entrambe utilizzabili anche a fini di trasferimenti di dati in Paesi terzi; in questo contesto, il regolamento assegna alle Autorità di controllo un ruolo non escluso di monitoraggio dell'attuazione e del rispetto di codici deontologici e schemi di certificazione, lasciando spazio anche a soggetti privati a ciò abilitati o accreditati.

In generale le disposizioni del Regolamento trovano applicazione sia per trattamenti automatizzati sia per trattamenti non automatizzati di dati personali.

È opportuno precisare che la protezione dei dati, come prevista dal Regolamento, sia applicata alle persone fisiche a prescindere dalla loro nazionalità o dal luogo di residenza. Il Regolamento, infatti, non disciplina il trattamento dei dati personali relativi alle persone giuridiche, in particolare imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto.

Il titolare del trattamento potrà quindi escludere la propria responsabilità solo adottando un corretto approccio al trattamento dei dati con cui è venuto in contatto, approccio che dovrà essere il più possibile rigoroso e conforme alle regole dettate non solo dal Regolamento UE 2016/679 ma anche dalla normativa nazionale ove applicabile e non direttamente in contrasto con le disposizioni contenute nel Regolamento stesso.

**Casi di esclusione dell'applicazione del Regolamento UE 2016/679**

Il Regolamento UE 2016/679 all'art. 2 2°co. prevede dei casi nei quali il Regolamento sulla protezione dei dati non si applica e per i quali, quindi, è consentito un uso libero del dato. Questi casi nello specifico sono:

1. i trattamenti effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione. Infatti, non si applica a questioni di tutela dei diritti e delle libertà fondamentali o di libera circolazione dei dati personali riferite ad attività che non rientrano nell'ambito di applicazione del diritto dell'Unione, quali le attività riguardanti la sicurezza nazionale, la politica estera ovvero la sicurezza comune dell'Unione;
2. i trattamenti effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico e quindi senza una connessione con un'attività commerciale o professionale;
3. i trattamenti effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse;
4. il regolamento non si applica al trattamento di informazioni anonime, anche per finalità statistiche o di ricerca;
5. il regolamento non si applica al trattamento dei dati personali delle persone decedute. Sul punto però va precisato che gli stati membri possono prevedere norme riguardanti il trattamento dei dati personali delle persone decedute e nello specifico in Italia il decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 n. 101/2018 ha previsto, all'art. art. 2 terdecies co. 1, che i diritti concernenti i dati personali delle persone decedute 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;
6. il regolamento non disciplina il trattamento dei dati personali relativi alle persone giuridiche, in particolare imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto.

## 2.0 Principi del Reg. UE 2016/679

La disciplina dei principi della protezione dei dati si sviluppa su piani differenti. Ci sono disposizioni generali sui principi (art. 5 Reg. UE 2016/679) e disposizioni specifiche sui principi (art. 6-11 Reg. UE 2016/679). Queste ultime possono riguardare categorie di dati o di soggetti oppure possono raggrupparsi in base al loro oggetto (i.e. adempimenti nei confronti degli interessati, adempimenti organizzativi, adempimenti di sicurezza). Le disposizioni generali sui principi hanno una valenza che copre ogni aspetto della disciplina e devono essere rispettate in ogni fase dello sviluppo del trattamento dei dati. I principali principi individuati dal Regolamento UE sono i seguenti:

a. **Liceità**: rispetto delle norme, è lecito un trattamento che non violi norme generali e norme specifiche dell'ordinamento;
b. **Correttezza**: rispetto di norme etiche, deontologiche non "codificati"; sono accorgimenti per rendere equilibrate le singole posizioni adeguando il trattamento alle esigenze reciproche, oltre allo stretto dato normativo;
c. **Trasparenza**: Assicurare la consapevolezza dell'interessato; quest'ultimo deve poter contare sul fatto che il titolare non metterà il velo sul trattamento, il dato deve essere sempre tracciabile da parte dell'interessato, significa, quindi, modalità operative che tengano conto della possibilità di *disclosure* in ogni momento da parte dell'interessato e ciò implica anche predisposizione organizzativa e di strumenti per eseguire la *disclosure;*
d. **Limitazione della finalità**: gli scopi del trattamento devono essere determinati, espliciti e legittimi, trattamenti successivi a quelli iniziali non devono avere finalità incompatibile a quella originaria (salvi gli ulteriori trattamenti per finalità di archiviazione nel pubblico interesse o per finalità di ricerca scientifica e storica o per finalità statistiche). Il rispetto del principio di finalità assume il significato di obbligazione contrattuale o di identificazione dei confini dell'attività istituzionale degli enti pubblici. Andare oltre le finalità significa inadempimento o sviamento;
e. **Minimizzazione dei dati**: i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità. Il principio di minimizzazione ha efficacia trasversale e implica una riduzione al minimo del numero dei dati, del tipo di trattamento, del soggetto che a vario titolo possono avere contezza dei dati, del periodo di conservazione. Determinante per la "minimizzazione" è l'esplicitazione delle finalità, pertanto la "minimizzazione" deve essere oggettiva, non conta la percezione soggettiva del titolare del trattamento, ma una relazione oggettiva tra finalità e dati utili;
f. **Esattezza**: i dati devono essere esatti e, se necessario, aggiornati; devono essere prese tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti. Il canone dell'esattezza del dato è di relativa facile applicazione per i dati oggettivi (che possono essere "veri" o "falsi"), mentre è di impossibile applicazione per i dati soggettivi (i.e. la profilazione). Per i dati soggettivi, la valutazione più congrua è quella della correttezza. Nel concetto di esattezza rientra anche quella di aggiornamento di dati un tempo esatti e non più tali e di integrazione di dati un tempo completi e non più tali per sopravvenuta lacunosità;
g. **Limitazione della conservazione**: i dati devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco temporale non superiore al conseguimento delle finalità per le quali sono trattati (salvo trattamenti di archiviazione nel pubblico interesse o per finalità di ricerca scientifica e storica o per finalità statistiche). Unitamente al tempo della conservazione è di dirimente importanza l'individuazione di modalità di conservazione distinte in relazione alle diverse fasi del trattamento;

h. **Integrità e riservatezza**: i dati devono essere trattati in modo 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. Il dato va protetto, perché solo attraverso la protezione dei dati si proteggono le persone fisiche a cui il dato si riferisce;

*i.* **Responsabilizzazione**: concetto che esprime l'attribuzione al titolare del trattamento l'obbligo giuridico di osservare il Regolamento e dell'onere processuale della prova di averlo fatto. È opportuno stabilire 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. In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficacie ed essere in grado di dimostrazione la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure stesse. 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.

Il Regolamento conferma che ogni trattamento deve trovare fondamento in un'idonea **base giuridica**, i fondamenti di liceità del trattamento sono indicati all'art. 6 del Regolamento UE 2016/679. Le condizioni di liceità, che sono trattate tutte insieme ovvero senza distinzione tra titolari del trattamento (enti pubblici / soggetti privati), possono essere distinte in due macro-categorie: quelle che richiedono il consenso dell'interessato e quelle che prescindono dal consenso dell'interessato.
La prima categoria - trattamenti che richiedono il consenso - ha una struttura contrattuale e consiste nell'incontro di volontà, la seconda - trattamenti che non richiedono il consenso - ha una struttura esclusivamente normativa e consiste nell'applicazione di una legge.
Nel primo caso l'interessato deve manifestare la sua opinione sul singolo trattamento; nel secondo caso l'interessato può solo tutelarsi *ex post* se il trattamento non rispetta lo standard normativo. Si noti che la seconda categoria - trattamenti senza consenso - non riguarda solo il settore della Pubblica Amministrazione mentre la categoria dei trattamenti che richiedono il consenso è appannaggio del settore dei titolari di trattamento privato.
Si procede ad analizzare ora le varie ipotesi in cui il trattamento è consentito, si deve però, sin d'ora precisare che per quei trattamenti per i quali è escluso il consenso, la trasparenza assume un ruolo essenziale nella catena delle garanzie per la persona fisica.

**1. Consenso al trattamento:**

si tratta della manifestazione di volontà relativa al trattamento e non al rapporto sostanziale soprastante.
L'articolo 4 del Regolamento UE definisce il consenso come qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.
L'istituto del consenso è cruciale per il trattamento dei dati; infatti, rappresenta una condizione legittimante per il trattamento dei dati. Il considerando n. 32, ad esempio, si occupa delle modalità di espressione e prefigura il consenso come un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio con dichiarazione scritta, anche attraverso mezzi elettronici o orale. Pertanto, potrebbe essere considerata espressione di consenso la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non potrebbe pertanto considerare assenso il silenzio, l'inattività o la preselezione di caselle. Il

consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o per le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale è espressa.

Il considerando n. 42 distribuisce l'onere della prova e grava il titolare del trattamento che, qualora il trattamento dei dati sia basato sul consenso, dovrebbe essere in grado di dimostrare che l'interessato ha acconsentito al trattamento. Ai fini del consenso informato, l'interessato dovrebbe essere posto a conoscenza almeno dell'identità del titolare del trattamento e delle finalità del trattamento cui sono destinati i dati personali. Il consenso non dovrebbe essere considerato liberamente espresso se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio.

Si presume che il consenso non sia stato liberamente espresso se non è possibile esprimere un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso, o se l'esecuzione di un contratto, compresa la prestazione di un servizio, è subordinata al consenso sebbene esso non sia necessario per tale esecuzione.

L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca non pregiudica la liceità del trattamento basata sul consenso prima dell'avvenuta revoca. Prima di esprimere il proprio consenso, l'interessato deve essere informato di ciò e, pertanto, il consenso è revocabile con la stessa facilità con cui viene prestato.

Per le particolari categorie di dati (i.e. dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona) l'art. 9 1° co. del Regolamento UE 2016/679 dispone il divieto di trattamento. Tra le cause esclusive del divieto, il 2° co. del medesimo articolo, viene indicato il caso in cui l'interessato abbia prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto.

Analizzando la normativa si evidenziano i seguenti indicatori di rischio:

a. le modalità formali non soddisfano il requisito della inequivocabilità;
b. il titolare unilateralmente qualifica come consenso il silenzio o l'inattività dell'interessato la preselezione di caselle;
c. la formula del consenso non è chiaramente distinguibile, ovvero non è contenuta in una clausola specifica separata dalle altre clausole del contratto o da altri contenuti;
d. la formula del consenso non è evidente dalla sua conformazione grafica: occorre inserire elementi di contenuto/forma che a un semplice sguardo evidenziano che lì si parla del diritto di dire di "sì" o di "no";
e. la formula del consenso deve utilizzare un linguaggio semplice e chiaro: tali requisiti vanno adeguati alla platea degli interessati di cui si tratta nella singola operazione - può essere necessario un linguaggio colloquiale e senza termini giuridici-;
f. non c'è espressamente scritto che il consenso può essere revocato e non è indicata la modalità di revoca, che deve essere semplice come manifestare il consenso; la revoca deve essere incondizionata;
g. non sono indicate l'identità del titolare del trattamento e le finalità del trattamento cui sono destinati i dati personali.

**2. Esistenza di un contratto o di trattative pre-contrattuali**

Il Regolamento UE ribadisce una regola di favore per le relazioni economiche. L'esistenza di una fase pre-contrattuale o di un contratto implica uno scambio di volontà sul rapporto soprastante ritenuto assorbente rispetto allo scambio di volontà

necessario per il trattamento dei dati. L'ambito di applicazione della norma è disegnato dalle finalità: la condizione auto legittimante (senza consenso dedicato al trattamento dei dati) vale solo negli stretti confini di quanto necessario per rispondere al contraente, o probabile contraente, e per eseguire il contratto. Nei contratti e nei pre-contratti, il consenso "privacy" è assorbito dal consenso "contrattuale" e ciò nei limiti delle prestazioni dedotte nel contratto. Il consenso autonomo gioca un ruolo imprescindibile nelle situazioni in cui non c'è un altro rapporto basato sul consenso o si va al di là di un altro rapporto basato sul consenso.

In conclusione, il trattamento dovrebbe essere considerato lecito se è necessario nell'ambito di un contratto o ai fini della conclusione di un contratto.

**3. Esecuzione di un obbligo legale e salvaguardia di interessi vitali**

È opportuno che il trattamento effettuato in conformità a un obbligo legale al quale il titolare del trattamento è soggetto o necessario per l'esecuzione di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri, sia basato sul diritto dell'Unione o di uno Stato membro. Il Regolamento non impone che vi sia un atto legislativo specifico per ogni singolo trattamento. Un atto legislativo può essere sufficiente come base per più trattamenti effettuati conformemente a un obbligo legale cui è soggetto il titolare del trattamento o se il trattamento è necessario per l'esecuzione di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri. Dovrebbe altresì spettare al diritto dell'Unione o degli Stati membri stabilire la finalità del trattamento. Inoltre, tale atto legislativo potrebbe precisare le condizioni generali del presente regolamento che presiedono alla liceità del trattamento dei dati personali, prevedere le specificazioni per stabilire il titolare del trattamento, il tipo di dati personali oggetto del trattamento, gli interessati, i soggetti cui possono essere comunicati i dati personali, le limitazioni delle finalità, il periodo di conservazione e altre misure per garantire un trattamento lecito e corretto. Dovrebbe spettare altresì al diritto dell'Unione o degli Stati membri stabilire se il titolare del trattamento che esegue un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri debba essere una pubblica autorità o altra persona fisica o giuridica di diritto pubblico o, qualora sia nel pubblico interesse, anche per finalità inerenti alla salute, quali la sanità pubblica e la protezione sociale e la gestione dei servizi di assistenza sanitaria, di diritto privato, quale un'associazione professionale.

Il trattamento dei dati è altresì considerato lecito quando è necessario per proteggere un interesse essenziale per la vita dell'interessato o un'altra persona fisica. Il trattamento di dati personali fondato sull'interesse vitale di un'altra persona fisica dovrebbe avere luogo in principio unicamente quando il trattamento non può essere manifestamente fondato su un'altra base giuridica. Ad esempio, alcuni trattamenti di dati personali possono rispondere sia a rilevanti motivi di interesse pubblico sia agli interessi vitali dell'interessato.

**4. Legittimo interesse del titolare**

In relazione a tale tipologia di condizione necessaria per il trattamento dei dati, il Garante per la protezione dei dati personali ha precisato che il bilanciamento fra legittimo interesse del titolare o del terzo e diritti e libertà dell'interessato non spetta all'Autorità ma è compito dello stesso titolare del trattamento, si tratta di una delle principali espressioni del principio di "responsabilizzazione" introdotto dal nuovo pacchetto protezione dati.

L'interesse legittimo del titolare del trattamento o del terzo deve, quindi, prevalere sui diritti e le libertà fondamentali dell'interessato per costituire un valido fondamento di liceità. Il Regolamento UE chiarisce espressamente che l'interesse legittimo del titolare del trattamento non costituisce idonea base giuridica per i trattamenti svolti dalle autorità pubbliche in esecuzione dei rispettivi compiti.

L'opinione adottata dal Gruppo Article 29 Data Protection Working Party del 9 aprile 2014 interpreta il concetto del bilanciamento previsto dal Regolamento UE e esemplifica alcuni trattamenti per i quali il criterio del legittimo interesse del

titolare del trattamento è applicabile. Nello specifico l'Opinion 06/2014 esprime il seguente principio "the legitimate interests of the controller (or third parties) must be balanced against the interests of fundamental rights and freedom of the data subject". La citata Opinion 06/2014 elenca esemplificativamente e senza pretesa di esaustività, alcuni contesti in cui potrebbe emerge un legittimo interesse del titolare del trattamento:

a. libertà di stampa e di espressione;
b. marketing diretto;
c. comunicazione politica;
d. campagne di raccolta fondi delle organizzazioni non lucrative;
e. recupero crediti anche stragiudiziale;
f. prevenzione frodi, antiriciclaggio;
g. controllo indiretto dei lavoratori;
h. segnalazione di illeciti (whistleblowing);
i. sicurezza fisica;
j. sicurezza informatica e delle reti;
k. ricerca storica, scientifica e statistica;
l. ricerche di mercato (comprese anche di marketing).

Il legittimo interesse potrebbe essere anche di terzi, ad esempio la citata Opinion 06/2014 sostiene che la pubblicazione di dati per scopi di trasparenza societaria (compensi degli amministratori) avvenga nell'interesse dei soci, della stampa e del pubblico interesse.

Per eseguire il bilanciamento, in primo luogo è importante considerare la natura e l'origine degli interessi legittimi e se il trattamento è necessario per perseguire quelli interessi, da un lato, e l'impatto sugli interessati. Fattori chiave da considerare quando si applica il bilanciamento sono:

- la natura e l'origine del legittimo interesse;
- l'impatto sui soggetti dati, tra cui:
    - la natura dei dati, ad esempio se il trattamento comporta dati che possono essere considerati riservati o sono stati ottenuti da fonti pubblicamente disponibili;
    - il modo in cui dati vengono elaborati, anche se i dati sono disponibili pubblicamente o altrimenti resi accessibili a un gran numero di persone, o se grandi quantità di dati personali sono elaborati o combinati con altri dati (i.e. in caso di profilazione, fini commerciali, l'applicazione della legge o altro);
    - le ragionevoli aspettative della persona interessata, specialmente per quanto riguarda l'uso e la divulgazione dei dati nel contesto pertinente;
    - lo stato del titolare e del soggetto di dati, tra cui l'equilibrio di potere tra la persona interessata e il titolare del trattamento, o se l'interessato è un minore altrimenti appartiene ad un segmento più vulnerabile della popolazione.
- Ulteriori misure di salvaguardia per prevenire indebiti impatti sui dati, tra cui:
    - minimizzazione dei dati (i.e. rigorose limitazioni sulla raccolta di dati, o di cancellazione immediati dei dati dopo l'uso);
    - misure tecniche e organizzative per garantire che i dati non possono essere utilizzati per prendere decisioni o altre azioni in relazione ai singoli individui;

- ampio uso di tecniche di anonimizzazione, aggregazione dei dati, tecnologie di rafforzamento della privacy, privacy by design, privacy e valutazioni di impatto di protezione dei dati.

Il Regolamento UE considera il legittimo interesse quale presupposto in cui si riversa l'assunzione di responsabilità - la responsabilizzazione del titolare - al pari del consenso e delle altre condizioni di liceità, soggetto a particolare trasparenza da valorizzare in maniera autonoma nelle varie informative.
Va precisato che il Gruppo Europeo dei Garanti (EDPB) ha adottato una nuova versione della Opinion 06/2014, ad oggi in corso di consultazione. La nuova versione dell'Opinion (Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR) quantomeno in questa sua versione non definitiva, mantiene comunque continuità con i concetti espressi e le prescrizioni adottate nell'Opinion 06/2014, senza stravolgimenti.

## 3.0 Dati appartenenti a categorie particolari ai sensi del Reg. UE 2016/679

Il Regolamento UE 2016/679 attribuisce una specifica protezione ai dati personali cd "particolari" che, per loro natura, sono particolarmente sensibili. Sono tali i dati personali che sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali dell'interessato.
Infatti, ai sensi dell'art. 6 1°co. Regolamento UE 2016/679, è sancito un divieto generale nel trattamento dei dati personali che rilevino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
Tra tali dati dovrebbero essere compresi anche i dati personali che rilevano l'origina razziale o etnica, ad esempio, il trattamento di fotografie non dovrebbe costituire sistematicamente un trattamento di particolari categorie di dati personali, poiché essere rientrano nella definizione di dati biometrici soltanto quando sono trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica.
Tali dati personali non dovrebbero essere oggetto di trattamento, a meno che il trattamento non sia consentito nei casi specifici di cui al 2° co. dell'art. 9 Regolamento UE 2016/679. È doveroso precisare che, in relazione al trattamento di tali dati, il Regolamento UE prevede che ogni Stato membro abbia il diritto di stabilire delle disposizioni specifiche sulla protezione dei dati per adeguare l'applicazione delle norme del Regolamento UE ai fini della conformità ad un obbligo legale o all'esecuzione di un compito di interesse pubblico o per l'esercizio di pubblici poteri di cui è investito il titolare del trattamento.
La deroga al divieto di trattare categorie particolari di dati personali dovrebbe essere consentita anche quando è prevista dal diritto dell'Unione o degli Stati membri, fatte salve adeguate garanzie, per proteggere i dati e altri diritti fondamentali, laddove ciò avvenga nell'interesse pubblico, in particolare il trattamento dei dati personali nel settore del diritto del lavoro e della protezione sociale, comprese le pensione, e per finalità di inerenti alla salute, compresa la sanità pubblica e la gestione dei servizi di assistenza sanitaria. La deroga al divieto generale di trattare categorie particolari di dati personali dovrebbe anche consentire di trattare tali dati personali, se necessari, per accertare, esercitare o difendere un diritto, che sia in sede giudiziaria, amministrativa o stragiudiziale.

Il Regolamento UE 2016/679 considera effettuato per motivi di interesse pubblico il trattamento dei dati personali, tra gli altri, quello a cura di autorità pubbliche allo scopo di realizzare fini, previsti dal diritto Costituzionale o dal diritto Internazionale Pubblico. Tale trattamento deve però essere proporzionato alle finalità perseguite, 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.
L'articolo 10 del Regolamento UE prescrive invece cautele ancora maggiori nel caso di trattamento di dati personali relativi a condanne penali, a reati o misure di sicurezza, che "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."
Non è quindi sufficiente una autorizzazione normativa al trattamento di tali dati, la prescrizione deve essere accompagnata da adeguate garanzie che chi effettua il trattamento è tenuto a porre in essere.

## 4.0 Le figure previste dal Reg. UE 2016/679

Il Regolamento UE 2016/679 prevede principalmente 5 figure ai cui rivolgere i propri principi e le proprie regole, queste figure sono: l'interessato, il titolare del trattamento, il responsabile del trattamento, il responsabile per la protezione dei dati (DPO) e l'autorità di controllo.

Di seguito si svilupperà una breve disamina di ogni figura con un particolare *focus* sui diritti e i doveri previsti in capo agli stessi dal Regolamento UE 2016/679.

## 4.1 L'interessato e i suoi diritti

All'interessato, alla cui definizione si rimanda, in conformità a quanto stabilito nel Regolamento UE 2016/679 artt. 12-23 vengono riconosciuti una serie di diritti in relazione al trattamento dei suoi dati, tali diritti sono:

1. Ai sensi dell'art. 15 Regolamento UE 2016/679, l'interessato **ha il diritto di ottenere la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e il relativo accesso** ai dati e alle seguenti informazioni:
   a) finalità del trattamento;
   b) categorie di dati personali in questione;
   c) destinatari dei dati, in particolare se sono Paesi terzi o Organizzazioni Internazionali;
   d) il periodo di conservazione dei dati o il criterio utilizzato per determinare questo periodo;
   e) l'esistenza del diritto alla rettificazione, cancellazione, limitazione del trattamento e di opposizione;
   f) diritto di proporre reclamo all'autorità di controllo;
   g) se i dati non sono raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
   h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione.

L'interessato dovrebbe ricevere le informazioni relative al trattamento dei dati personali che lo riguardano al momento della raccolta presso l'interessato o, se i dati sono stati ottenuti da altra fonte, entro un termine ragionevole, in funzione

delle circostanze del caso. Se i dati personali possono essere legittimamente comunicati a un altro destinatario, l'interessato dovrebbe esserne informato nel momento in cui il destinatario riceve la prima comunicazione dei dati personali. L'interessato dovrebbe, inoltre, poter accedere ai dati personali raccolti che lo riguardando ed esercitare facilmente tale diritto ad intervalli ragionevoli, per essere consapevole del trattamento e verificarne la liceità.

2. **Diritto alla rettifica e cancellazione**: l'interessato ha 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 diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

In generale, con riferimento a tutte le ipotesi di rettificazione (aggiornamento, integrazione e correzione) va stabilito in concreto se il risultato è una doppia informazione o una sola e cioè quella risultante dalla rettifica. In altre parole, si deve tenere l'informazione iniziale cui si aggiunge l'informazione rettificata, l'informazione integrativa e l'informazione aggiornata. Il mantenimento della doppia informazione potrebbe anche essere imposto dalla legge o rispondente alla tutela dell'interessato o comunque coerente con le finalità e le modalità di trattamento.

Si sottolinea, infine, che l'interessato che desideri rettificare i propri dati lo deve richiedere espressamente.

L'art. 17 del Regolamento UE 2016/679 disciplina il diritto alla cancellazione dei dati in capo all'interessato, ovvero il c.d. diritto all'oblio.

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

- i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
- l'interessato revoca il consenso precedentemente prestato a quel determinato trattamento, salvo non sussista altro fondamento giuridico per il trattamento;
- l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento;
- i dati personali sono stati trattati illecitamente;
- i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione 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.

Vi sono, tuttavia, una serie di casi per i quali non è concesso all'interessato la facoltà di esercitare il proprio diritto alla cancellazione dei dati in quanto, il trattamento viene considerato necessario in relazione a:

- l'esercizio del diritto alla libertà di espressione e di informazione;
- l'adempimento di un obbligo legale 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;
- motivi di interesse pubblico nel settore della pubblica sanità;
- fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, nella misura in cui l'esercizio del diritto alla cancellazione rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;
- l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Si sottolinea, infine, che l'interessato che desideri cancellare i propri dati lo deve richiedere espressamente.

3. **Diritto alla limitazione del trattamento:** ai sensi dell'art. 18 Regolamento UE 2016/679, l'interessato ha diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:
   a. l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;
   b. il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
   c. benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
   d. l'interessato si è opposto al trattamento, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

Le modalità per limitare il trattamento dei dati personali potrebbero consistere, tra l'altro, nel trasferire temporaneamente i dati selezionati verso un altro sistema di trattamento, nel rendere i dati personali selezionati inaccessibili o nel rimuovere temporaneamente i dati pubblicati da un sito web. Negli archivi automatizzati, la limitazione del trattamento dei dati personali dovrebbe, in linea di massima, essere assicurata mediante dispositivi tecnici in modo tale che i dati personali non siano sottoposti a ulteriore trattamento e non possano più essere modificati. Il sistema dovrebbe indicare chiaramente che il trattamento dei dati è stato limitato.

Il diritto di limitazione del trattamento, tuttavia, non si applica quando il trattamento viene svolto comunque con il consenso dell'interessato ovvero 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.

4. **Diritto alla portabilità dei dati:** per rafforzare ulteriormente il controllo sui propri dati è opportuno che l'interessato abbia il diritto, qualora i dati personali siano trattati con mezzi automatizzati, di ricevere in un formato strutturato, di uso comune, leggibile da dispositivo automatico e interoperabile i dati personali che lo riguardano che abbia fornito a un titolare del trattamento e di trasmetterli a un altro titolare del trattamento. È opportuno che i titolari del trattamento sviluppino e utilizzino formati interoperabili che consentano la portabilità dei dati.

Tale diritto dovrebbe applicarsi qualora l'interessato abbia fornito i dati personali sulla base del proprio consenso o se il trattamento è necessario per l'esecuzione di un contratto. Non dovrebbe applicarsi qualora il trattamento si basi su un fondamento giuridico diverso dal consenso o contratto. Per sua stessa natura, tale diritto non dovrebbe essere esercitato nei confronti dei titolari del trattamento che trattano dati personali nell'esercizio delle loro funzioni pubbliche.

Il diritto alla portabilità dei dati non si applica qualora il trattamento dei dati sia necessario per l'adempimento di un obbligo legale 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.

Infine, l'esercizio di tale diritto da parte dell'interessato non dovrebbe pregiudicare il diritto dello stesso ad ottenere la cancellazione dei dati personali riguardanti l'interessato forniti da quest'ultimo per l'esecuzione di un contratto, nella misura in cui e fintantoché i dati siano necessari all'esecuzione del tale contratto. Ove tecnicamente fattibile, l'interessato dovrebbe avere il diritto di ottenere che i dati personali siano trasmessi direttamente da un titolare del trattamento ad un altro.

5. **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, compresa la profilazione. Il titolare del trattamento, quindi, 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.

6. **La profilazione e il processo decisionale automatizzato:** 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.

Tale trattamento comprende la profilazione, che consiste in una forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato, ove ciò produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona.

Tuttavia, è opportuno che sia consentito adottare decisioni sulla base di tale trattamento, compresa la profilazione, se ciò è espressamente previsto dal diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento, anche ai fini di monitoraggio e prevenzione delle frodi e dell'evasione fiscale secondo i regolamenti, le norme e le raccomandazioni delle istituzioni dell'Unione o degli organismi nazionali di vigilanza e a garanzia della sicurezza e dell'affidabilità di un servizio fornito dal titolare del trattamento o, se necessario, per la conclusione o l'esecuzione di un contratto tra l'interessato e il titolare del trattamento, o se l'interessato ha espresso il proprio consenso esplicito.

In ogni caso, tale trattamento - la profilazione - dovrebbe essere subordinato a garanzie adeguate, che dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione.

Al fine di garantire un trattamento corretto e trasparente nel rispetto dell'interessato, tenendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono stati trattati, è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impedisca tra l'altro effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero che comportano misure aventi tali effetti. Il processo decisionale automatizzato e la profilazione basati su categorie particolari di dati personali dovrebbero essere consentiti solo a determinate condizioni per quali il Regolamento UE 2016/679 rimanda alle norme degli Stati membri.

7. **Limitazioni:** Ai sensi dell'art 23 Regolamento UE 2016/679 il diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o il responsabile del trattamento può limitare, mediante misure legislative, la portata degli obblighi e dei diritti di cui agli articoli da 12 a 22 e 34, nonché all'art. 5 del Regolamento UE 2016/679, nella misura in cui le disposizioni ivi contenute corrispondano ai diritti e agli obblighi di cui agli articoli da 12 a 22.

Il diritto dell'Unione o degli Stati membri può imporre limitazioni a specifici principi e ai diritti di informazione, accesso, rettifica e cancellazione dei dati, al diritto alla portabilità dei dati, al diritto di opporsi, alle decisioni basate sulla profilazione, nonché alla comunicazione di una violazione di dati personali all'interessato e ad alcuni obblighi connessi in capo ai titolari del trattamento ove ciò sia necessario e proporzionato in una società democratica per la salvaguardia della sicurezza pubblica, ivi comprese la tutela della vita umana, le attività di prevenzione, indagine e perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione contro minacce alla pubblica sicurezza, per la tutela di importanti

obiettivi di interesse pubblico generale dell'Unione o di uno degli Stati membri, tra cui un interesse economico o finanziario rilevante dell'Unione o dello Stato membro stesso, per la tenuta di registri pubblici per ragioni di interesse pubblico generale o per l'ulteriore trattamento di dati personali archiviati.

8. **Reclamo:** Ciascun interessato dovrebbe avere il diritto di proporre reclamo, fatto salvo ogni altro ricorso amministrativo o giurisdizionale, quando ritenga che il trattamento che lo riguarda violi il Regolamento UE 2016/679 a un'autorità di controllo, segnatamente nello Stato membro in cui risiede abitualmente, lavora oppure del luogo dove si è verificata la presunta violazione.
9. **Ricorso giurisdizionale verso l'autorità di controllo:** fatto salvo ogni altro ricorso amministrativo o extragiudiziale, ogni persona fisica ha il diritto di proporre un ricorso giurisdizionale effettivo avverso una decisione giuridicamente vincolante dell'autorità di controllo. L'interessato, altresì, ha il diritto di proporre un ricorso giurisdizionale nei confronti dell'autorità di controllo anche qualora la stessa non tratti un reclamo o non lo informi entro tre mesi dello stato o dell'esito del reclamo proposto dall'interessato stesso. Le azioni nei confronti dell'autorità di controllo sono proposte dinanzi alle autorità giurisdizionali dello Stato membro in cui l'autorità di controllo è stabilita.

**Ricorso giurisdizionale nei confronti del titolare o del responsabile del trattamento:** fatto salvo ogni altro ricorso amministrativo o extragiudiziale disponibile, compreso il reclamo promosso avanti ad un'autorità di controllo, ogni interessato ha il diritto di proporre un ricorso giurisdizionale effettivo qualora ritenga che i diritti di cui gode a norma del Regolamento UE 2016/679 siano stati violati a seguito di un trattamento. Le azioni nei confronti del titolare del trattamento o del responsabile del trattamento sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui il titolare del trattamento o il responsabile del trattamento ha uno stabilimento. In alternativa, tali azioni possono essere promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'interessato risiede abitualmente, salvo che il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica di uno Stato membro nell'esercizio dei pubblici poteri.

## 4.2 Il Titolare del trattamento

Con il Regolamento UE 2016/679 è stata stabilita 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. In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguati ed efficaci, nonché essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.

La tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede, quindi, l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento. Al fine di poter dimostrare la conformità con il Regolamento UE 2016/679, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di *default*. Tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, pseudonimizzare i dati personali il più presto possibile, offrire trasparenza per quando riguarda le funzioni e il trattamento dei dati personali, consentire all'interessato di controllare il trattamento dei dati e consentire al titolare del trattamento di creare e migliorare caratteristiche di sicurezza. In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento dei dati personali o che trattano dati personali per svolgere le loro

funzioni, i produttori di prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del titolare e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati. I principi della protezione dei dati fin dalla progettazione e di *default* dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici.

Alla luce di quanto sopra detto, si possono riassumere i principi di novità introdotti con il Regolamento UE 2016/679 nei seguenti:

- **Accountability**: disciplinata all'art. 24 del Regolamento UE 2016/679, si compone di tre aspetti:
  - **(i)** **Trasparenza:** accessibilità alle informazioni
  - **(ii)** **Rendiconto:** per rispondere agli *stakeholder*
  - **(iii)** **Responsabilità:** capacità di far rispettare le norme e le regole di comportamento ai titolari del trattamento

Quando si parla di a*ccountability* si deve tenere conto della natura, del campo di applicazione, del contesto, delle finalità del trattamento, dei rischi. Su queste basi, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire e riuscire a dimostrare che il trattamento dei dati è in conformità al Regolamento UE 2016/679. Le misure adottate di tanto in tanto vanno riesaminate e se necessario aggiornate.

- **Privacy by design e by default:** disciplinati all'art. 25 del Regolamento UE 2016/679 sono due principi con carattere di novità assoluta rispetto agli adempimenti a cui il titolare del trattamento era tenuto prima dell'introduzione del nuovo Regolamento UE, nel dettaglio:
  - **(i)** **Privacy by design:** attuazione di adeguate misure di protezione dei dati con tecniche organizzative sin dal momento della progettazione che dell'esecuzione del trattamento stesso per garantire il rispetto del Regolamento. Ciò significa, in altre parole, che la protezione dei dati sia integrata nell'intero ciclo di vita della tecnologia: progettazione, distribuzione, uso, eliminazione;
  - **(ii)** **Privacy by default:** il titolare deve garantire che siano trattati di *default* solo i dati personali necessari per la finalità specifica del trattamento e che la quantità e la durata dei dati sia minima, si cerca di limitare quindi: i dati trattati, il periodo di conservazione, l'accessibilità.

Il titolare può adottare dei codici di condotta oppure ottenere una certificazione dei propri sistemi al fine di dimostrare il rispetto degli obblighi in capo al titolare del trattamento e conformi al Regolamento UE 2016/679.

Tra le attività prioritarie a cui è chiamato il titolare del trattamento per la pianificazione e gestione dell'attività di protezione delle persone con riguardo al trattamento dei dati si richiama quanto disposto all'art. 30 del Regolamento UE 2016/679, nel quale viene disciplinato il registro dei trattamenti.

- **Registro dei trattamenti:** ai sensi dell'art. 30 Regolamento UE 2016/679 ogni titolare e, ove applicabile, il suo rappresentante tengono un registro delle attività svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:
  a. il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
  b. le finalità del trattamento;
  c. una descrizione delle categorie di interessati e delle categorie di dati personali;
  d. le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

e. ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'art. 49, la documentazione delle garanzie adeguate;
f. ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g. ove possibile, una descrizione generale delle misure d sicurezza tecniche e organizzative;

La disciplina qui richiamata in relazione ai doveri del titolare del trattamento è altresì applicabile anche al responsabile dei trattamenti, il quale è obbligato a tenere un registro di tutte le attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:

(i) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile per la protezione dei dati;
(ii) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
(iii) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma art. 49, la documentazione delle garanzie adeguate;
(iv) ove applicabile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Il Regolamento UE 2016/679 dispone che per la tenuta del registro dei trattamenti non si applichi alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'art. 9 1° co, o i dati personali relativi a condanne penali e a reati di cui all'art. 10 del Regolamento UE.

Tuttavia, anche in un'ottica di cooperazione fra i titolari del trattamento e l'Autorità di controllo, si consiglia la tenuta dei registri per il trattamento al fine di monitorare con precisione i trattamenti effettivamente effettuati.

Infine, si rende doveroso sottolineare che è necessario un aggiornamento periodico dei registri del trattamento e occorre che gli stessi siano coordinati con altri adempimenti documentali, quale le informative o altri atti che descrivono i trattamenti stessi (i.e. analisi dei rischi, la valutazione di impatto, istanze di consultazione preliminare). Sarebbe quindi utile considerare il registro dei trattamenti come una base dei dati iniziale dalla quale attingere l'apparato informativo per gli altri adempimenti.

- **Misure di sicurezza:** Il Regolamento UE 2016/679 prevede all'art. 32 una serie di misure di sicurezza che devono essere adottate dal titolare del trattamento. Si richiede, quindi, che il titolare del trattamento o il responsabile del trattamento valutino i rischi inerenti al trattamento e attuino le misure per limitare tali rischi, quali ad esempio la cifratura. Tali misure dovrebbero, in ogni caso, assicurare un adeguato livello di sicurezza, inclusa la riservatezza, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere. Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, 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.

Il titolare del trattamento, inoltre, dovrebbe essere responsabile dello svolgimento di una valutazione d'impatto sulla protezione dei dati per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio. L'esito della valutazione dovrebbe essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento è conforme a quanto richiesto e previsto del Regolamento UE stesso. Qualora la valutazione

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

Le misure tecniche che vengono individuate del Regolamento UE stesso sono:

(i) la pseudonimizzazione e la cifratura dei dati personali;

(ii) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

(iii) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

(iv) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso ai 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 Garante ha affermato che le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento *ex* art. 32 1° co., in questo caso la lista di cui al cennato articolo è una lista aperta e non esaustiva. Per lo stesso motivo, non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza ex art. 33 del D.Lgs. 196/2003 (Codice Privacy) poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificatamente individuati come affermato anche all'art. 32 del Regolamento UE 2016/679. Si richiama l'attenzione anche sulla possibilità di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate.

Tuttavia, facendo riferimento alle prescrizioni contenute, in particolare, nell'Allegato B al Codice Privacy, l'Autorità potrà valutare la definizione di linee guida o buone prassi sulla base dei risultati positivi conseguiti in questi anni; inoltre, per alcune tipologie di trattamenti (i.e. art. 6 1° co. lett. c) e e) del Regolamento UE 2016/679) potranno restare in vigore le misure di sicurezza attualmente previste attraverso le disposizioni di legge volta per volta applicabili: è il caso, in particolare, dei trattamenti dei dati sensibili svolti dai soggetti pubblici per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi, ove questi ultimi contengano disposizioni in materia di sicurezza dei trattamenti.

- **Data Breach:** La violazione dei dati personali è definita all'art. 4 del Regolamento UE 2016/679 come 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. Si tratta di un evento che va affrontato e gestito subito, al fine di evitare l'insorgenza o l'aggravamento di danni fisici, materiali o immateriali alle persone fisiche, come ad esempio:
  - perdita de controllo dei dati personali o limitazione dei loro diritti;
  - discriminazione, furto o usurpazione d'identità;
  - perdite finanziarie;
  - decifratura non autorizzata delle pseudonimizzazione;
  - pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale.

L'episodio pregiudizievole non deve quindi essere celato, poiché l'oscuramento della notizia, oltre a esporre a gravi sanzioni amministrative pecuniarie, amplifica gli effetti negativi dell'evento e inibisce forme di reazione pubblica e dell'interessato.

Sul punto all'art. 33 il Regolamento UE 2016/679 impone l'obbligo in capo al titolare del trattamento che, in caso di violazione dei dati personali, notifichi all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

La notifica della violazione dei dati personali all'autorità di controllo deve almeno:

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

Il titolare del trattamento deve, infine, documentare qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto della corretta procedura di segnalazione da parte del titolare del trattamento.

Inoltre, il titolare dovrebbe comunicare all'interessato la violazione dei dati personali senza indebito ritardo, qualora questa violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà della persona fisica, al fine di consentirgli di prendere le precauzioni necessarie. La comunicazione dovrebbe descrivere la natura della violazione dei dati personali e formulare raccomandazioni per la persona fisica interessata intese ad attenuare i potenziali effetti negativi. Tali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti dalle autorità stesse.

La comunicazione nei confronti dell'interessato non è richiesta quando è soddisfatta almeno una delle seguenti condizioni:

(i) 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 ad esempio la cifratura;
(ii) 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;
(iii) 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.

- **Valutazione d'impatto:** quando un tipo di trattamento, che prevede in particolare l'uso di nuove tecnologie, o in relazione alla sua natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi. Si precisa che la valutazione d'impatto sulla protezione dei dati, o la violazione d'impatto sulla protezione dei dati si riveli necessaria alla luce del tempo trascorso dal trattamento iniziale.

La valutazione di impatto dovrebbe vertere, in particolare, anche sulle misure, sulle garanzie e sui meccanismi previsti per attenuare i rischi in relazione ai trattamenti attuati e assicurando, di conseguenza, la protezione dei dati personali e dimostrando la conformità alle disposizioni previste dal Regolamento UE 2016/679.
La valutazione di impatto dovrebbe applicarsi in particolare ai trattamenti su larga scala, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato.
Alla luce di quanto detto e, in conformità a quanto espresso dal Regolamento UE 2016/679 all'art. 35, la valutazione di impatto è richiesta in particolare nei seguenti casi:

- una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- il trattamento su larga scala di particolari categorie di dati o di dati relativi a condanne penali e a reati;
- la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

La valutazione di impatto contiene almeno:

- una descrizione sistematica dei trattamenti previsti e della finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
- una valutazione delle necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità dei trattamenti al Regolamento UE 2016/679, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Se dalla valutazione d'impatto sulla protezione dei dati risulta che il trattamento, in mancanza delle garanzie, delle misure di sicurezza e dei meccanismi per attenuare il rischio, presenterebbe un rischio elevato per i diritti e le libertà delle persone fisiche e il titolare del trattamento è del parere che il rischio non possa essere ragionevolmente attenuato in termini di tecnologie disponibili e costi di attuazione, è opportuno consultare l'autorità di controllo. Tale rischio elevato potrebbe scaturire da certi tipi di trattamento e dall'estensione e frequenza del trattamento, da cui potrebbe derivare altresì un danno o un'interferenza con i diritti e le libertà della persona fisica. L'autorità di controllo che riceve una richiesta di consultazione dovrebbe darvi seguito entro un termine determinato. Tuttavia, la mancanza di reazione dell'autorità di controllo entro tale termine dovrebbe far salvo ogni intervento della stessa nell'ambito dei sui compiti e poteri previsti dal Regolamento UE 2016/679, compreso il potere di vietare i trattamenti. Nell'ambito di tale processo di consultazione, può essere presentato all'autorità di controllo il risultato di una valutazione d'impatto sulla protezione dei dati effettuata riguardo al trattamento in questione, in particolare le misure previste per attenuare il rischio per i diritti e le libertà delle persone fisiche.

- **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'art. 35 del Regolamento UE 2016/679 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare per attenuare il rischio.

Al momento di consultare l'autorità di controllo il titolare del trattamento comunica all'autorità stessa le seguenti informazioni:

- 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;

- le finalità e i mezzi del trattamento previsto;
- le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati in conformità al presente Regolamento UE;
- la valutazione d'impatto sulla protezione dei dati di cui all'art. 35 del Regolamento UE 2016/679;

ogni altra informazione richiesta dall'autorità di controllo.

## 4.3 Il Responsabile del trattamento

Per garantire che siano rispettate le prescrizioni del Regolamento UE 2016/679 quando il titolare del trattamento affida delle attività di trattamento a un responsabile del trattamento il titolare dovrebbe ricorrere unicamente a responsabili del trattamento 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 Regolamento UE 2016/679, anche per la sicurezza del trattamento.

L'applicazione da parte del responsabile del trattamento di un codice di condotta approvato o di un meccanismo di certificazione approvato può essere utilizzata come elemento per dimostrare il rispetto degli obblighi da parte del titolare del trattamento.

L'esecuzione dei trattamenti da parte del responsabile dovrebbe essere disciplinata da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri che vincoli il responsabile del trattamento al titolare del trattamento, in cui siano stipulati la materia disciplinata e la durata del trattamento, la natura e le finalità del trattamento, il tipo di dati personali e le categorie di soggetti interessati, tenendo conto dei compiti e responsabilità specifici del responsabile del trattamento nel contesto del trattamento da eseguire e del rischio in relazione ai diritti e alle libertà dell'interessato.

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

a. tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
b. garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
c. adotti tutte le misure di sicurezza richieste ai sensi dell'art. 32 del Regolamento UE 2016/679;
d. rispetti le condizioni di cui ai paragrafi 2 e 4 dell'art. 28 del Regolamento UE 2016/679 quando il responsabile ricorre a sua volta ad altro responsabile;
e. tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di are seguito alle richieste per l'esercizio dei diritti dell'interessato;
f. assista il titolare del trattamento nel compimento degli obblighi in capo allo stesso e concorrenti con il responsabile;

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

h. metta a disposizione del titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui è gravato e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato. Il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzioni violi il Regolamento UE 2016/679 o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

Fatto salvo un contratto individuale tra il titolare del trattamento e il responsabile del trattamento, il contratto o altro atto giuridico può basarsi, in tutto o in parte, su clausole contrattuali introdotte dell'autorità di controllo o dalla Commissione, anche laddove siano parte di una certificazione concessa al titolare del trattamento o al responsabile del trattamento stesso.

## 4.4 Il Responsabile della protezione dei dati

Per i trattamenti effettuali da un'autorità pubblica, eccettuate le autorità giurisdizionali o autorità giudiziarie indipendenti quando esercitano le loro funzioni giurisdizionali, o per i trattamenti effettuali nel settore privato da un titolare del trattamento le cui attività principali consistono in trattamenti che richiedono un monitoraggio regolare e sistematico degli interessati su larga scala, o ove le attività principali del titolare del trattamento o del responsabile del trattamento consistano nel trattamento su larga scala di categorie particolari di dati personali e di dati relativi alle condanne penali e ai reati, il titolare del trattamento o il responsabile del trattamento dovrebbe essere assistito da una persona che abbia una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati nel controllo del rispetto a livello interno del Regolamento UE 2016/679. Il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali trattati dal titolare del trattamento o dal responsabile del trattamento.

Tali responsabili della protezione dei dati, dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente.

Alla luce di quanto brevemente riassunto, il Regolamento UE 2016/679 dispone che 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 interessai 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 o di dati relativi a condanne penali e a reati.

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.

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

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, altresì, che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione dei compiti a lui assegnati. Il responsabile della protezione dei dati non può essere rimosso o penalizzato dal titolare del trattamento o dal responsabile per l'adempimento dei propri compiti (e per questo motivo sarebbe opportuno, nel caso di responsabile della protezione dei dati incaricato con contratto di servizi, che lo stesso abbia un incarico pluriennale, per consentire una effettiva acquisizione delle procedure aziendali e per evitare che il titolare possa esercitare una influenza sul responsabile della protezione dei dati facendo leva sul frequente rinnovo del contratto di servizi). Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.
Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:

(i) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento UE 2016/679 nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

(ii) sorvegliare l'osservanza del Regolamento UE 2016/679, 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;

(iii) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;

(iv) cooperare con l'Autorità di controllo;

(v) fungere da punto di contatto per l'Autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva come prevista ai sensi dell'art. 36 del Regolamento UE 2016/679, ed effettuare, se del caso, consultazione relativamente a qualunque altra questione.

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

## 4.5 Autorità di controllo

L'istituzione di autorità di controllo a cui è conferito il potere di eseguire i loro compiti ed esercitare i loro poteri in totale indipendenza in ciascuno Stato membro è un elemento essenziale della protezione delle persone fisiche con riguardo al trattamento dei loro dati personali.
Ogni Stato membro dispone che una o più autorità pubbliche indipendenti siano incaricate di svolgere l'applicazione del Regolamento UE 2016/679 al fine di tutelar ei diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione.
Ogni autorità di controllo agisce in piena indipendenza nell'adempimento dei propri compiti e nell'esercizio dei propri poteri conformemente al Regolamento UE 2016/679.
Sul proprio territorio ogni autorità di controllo:

(i) sorveglia e assicura l'applicazione del Regolamento UE 2016/679;

(ii) promuove la consapevolezza e favorisce la comprensione del pubblico riguardo ai rischi, alle norme, alle garanzie e ai diritti in relazione al trattamento. Sono oggetto di particolare attenzione le attività destinate specificatamente ai minori;

(iii) fornisce consulenza, a norma del diritto degli Stati membri, al parlamento nazionale, al governo e ad altri organismi e istituzioni in merito alle misure legislative e amministrative relative alla protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento;

(iv) promuove la consapevolezza dei titolari del trattamento e dei responsabili del trattamento riguardo agli obblighi imposti loro dal Regolamento UE 2016/679;

(v) su richiesta, fornisce informazioni all'interessato in merito all'esercizio dei propri diritti derivanti dal Regolamento UE 2016/679 e, se del caso, coopera a tal fine con le autorità di controllo di altri Stati membri;

(vi) tratta i reclami proposti da un interessato, o da un organismo, un'organizzazione o un'associazione ai sensi dell'art. 80 Regolamento UE 2016/679, e svolge le indagini opportune sull'oggetto del reclamo e informa il reclamante dello stato e dell'esito delle indagini entro un termine ragionevole, in particolare ove siano necessarie ulteriori indagini o un coordinamento con un'altra autorità di controllo;

(vii) collabora, anche tramite scambi di informazioni, con le autorità di controllo e presta assistenza reciproca al fine di garantire l'applicazione e l'attuazione coerente del Regolamento UE 2016/679;

(viii) svolge indagini sull'applicazione del Regolamento UE 2016/679, anche sulla base di informazioni ricevute da un'altra autorità di controllo o da un'altra autorità pubblica;

(ix) sorveglia gli sviluppi che presentano un interesse, se e in quanto incidenti sulla protezione dei dati personali, in particolare l'evoluzione delle tecnologie dell'informazione e della comunicazione e le prassi commerciali;

(x) svolge qualsiasi altro compito legato alla protezione dei dati personali.

## 5.0 Sanzioni previste dal Reg. UE 2016/679

Nelle azioni contro un titolare del trattamento o un responsabile del trattamento, il ricorrente può avviare un'azione legale dinanzi all'autorità giurisdizionale dello Stato membro in cui il titolare del trattamento o il responsabile del trattamento ha uno stabilimento o in cui risiede l'interessato, salvo che il titolare del trattamento sia un'autorità pubblica di uno Stato membro che agisce nell'esercizio dei suoi poteri pubblici.

Il titolare del trattamento o il responsabile del trattamento dovrebbe risarcire i danni cagionati a una persona da un trattamento non conforme alle disposizioni del Regolamento UE 2016/679, ma dovrebbe essere esonerato da tale responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile. Il concetto di danno dovrebbe essere interpretato in senso lato ed alla luce della giurisprudenza della Corte di Giustizia in modo tale da rispecchiare pienamente gli obiettivi del Regolamento UE 2016/679.

Ciò non pregiudica le azioni di risarcimento dei danni derivanti dalla violazione di altre norme del diritto dell'Unione o degli Stati membri.

Un trattamento non conforme al Regolamento UE 2016/679 comprende anche il trattamento non conforme agli atti delegati e agli atti di esecuzione adottati in conformità al Regolamento UE stesso e alle disposizioni degli Stati membri che specificano disposizioni del Regolamento.

Per rafforzare il rispetto delle norme contenute nel Regolamento UE 2016/679 sono state introdotte delle sanzioni, comprese sanzioni amministrative pecuniarie per violazione del Regolamento stesso, in aggiunta o in sostituzione di misure appropriate imposte dall'autorità di controllo ai sensi del Regolamento UE 2016/679.

Si deve prestare, in relazione all'applicazione della sanzione, attenzione alla natura, alla gravità e alla durata della violazione, al carattere doloso della violazione e alle misure adottate per attenuare il danno subito, al grado di responsabilità o eventuali precedenti violazioni pertinenti, alla maniera in cui l'autorità di controllo ha preso conoscenza della violazione, al rispetto dei provvedimenti disposti nei confronti del titolare del trattamento o del responsabile del trattamento, all'adesione a un codice di condotta ed eventuali altri fattori aggravanti o attenuanti. L'imposizione di sanzioni, comprese sanzioni amministrative pecuniarie dovrebbe essere soggetta a garanzie procedurali appropriate in conformità dei principi generali del diritto dell'Unione e della Carta, inclusi l'effettiva tutela giurisdizionale e il giusto processo.

Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte ai titolari del trattamento o ai responsabili del trattamento in conformità a quanto previsto dal Regolamento UE 2016/679, siano in ogni singolo caso effettive, proporzionate e dissuasive.

Al momento di infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso l'autorità di controllo tiene debito conto dei seguenti elementi:

a. la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o la finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;
b. il carattere doloso o colposo della violazione;
c. le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;
d. il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto;
e. eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;
f. il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuare i possibili effetti negativi;
g. le categorie di dati personali interessate dalla violazione;
h. la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare o il responsabile del trattamento ha notificato la violazione;
i. l'adesione ai codici di condotta approvati o ai meccanismi di certificazione approvati;
j. eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

Se, in relazione allo stesso trattamento o trattamenti collegati, un titolare del trattamento o un responsabile del trattamento viola, con dolo o colpa, varie disposizioni del Regolamento UE 2016/679, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave.

Si applica la sanzione amministrativa pecuniaria **fino a 10.000.000 Euro**, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente se superiore, in caso di violazione delle seguenti disposizioni:

(i) gli obblighi imposti dal Regolamento UE 2016/679 al titolare del trattamento o al responsabile del trattamento, come previste e disciplinate ai sensi degli artt. 8, 11, da 25 a 39, 42 e 43 del Regolamento UE 2016/679;

(ii) gli obblighi imposti dal Regolamento UE 2016/679 agli organismi di certificazione e di controllo.

Si applica la sanzione amministrativa pecuniaria **fino a 20.000.000 Euro**, o per le imprese, fino al **4% del fatturato** mondiale totale annuo dell'esercizio precedente se superiore, in caso di violazione delle seguenti disposizioni:

(i) i principi base del trattamento, comprese le condizioni relative al consenso, come previste e disciplinate ai sensi degli artt. 5, 6, 7 e 9 del Regolamento UE 2016/679;

(ii) i diritti degli interessati, come previsti e disciplinati ai sensi degli artt. da 12 a 22 del Regolamento UE 2016/679;

(iii) i trasferimenti di dati personali a un destinatario in un Paese terzo o un'Organizzazione Internazionale, come previsti e disciplinati ai sensi degli artt. da 44 a 49 del Regolamento UE 2016/679;

(iv) qualsiasi obbligo ai sensi delle legislazioni degli Stati membri in relazione alle disposizioni attuate dagli stessi per determinate tipologie di trattamenti, quali ad esempio: libertà d'espressione e di informazione, accesso del pubblico a documenti ufficiali, trattamento dei dati nell'ambito del rapporto di lavoro, come previste e disciplinate ai sensi degli artt. da 85 a 91 del Regolamento UE 2016/679;

(v) 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 come previsti e disciplinati ai sensi dell'art. 58 del Regolamento UE 2016/679.

## PARTE SPECIALE

### 1.0 Settori in cui opera l'azienda

Azienda Trasporti Funicolari Malcesine Monte Baldo è un Consorzio costituito nel 1955 per promuovere e sostenere il turismo sul lago di Garda.
Componenti del Consorzio sono la Provincia di Verona, la Camera di Commercio I.A.A. di Verona e il Comune di Malcesine.

Il Consorzio ha come oggetto principale l'impianto e l'esercizio di funivie per il trasporto di persone e cose ed in particolare della funivia che collega il capoluogo del Comune di Malcesine alla frazione di S. Michele e alla dorsale del Monte Baldo.

Il Consorzio si occupa però anche dell'impianto di risalita Prada-Costabella (di recente apertura) nonché di attività ancillari quali ad esempio la ristorazione (in riferimento allo Sky Walk Lounge Bar sito in prossimità della stazione di arrivo dell'impianto di risalita alla dorsale del Monte Baldo).

Il flusso di dati personali gestito dal Consorzio (che agisce per sua natura in massima parte quale autonomo titolare del trattamento) riguarda principalmente la gestione contrattuale del dato di fornitori e clienti, nonché la gestione contrattuale del dato dei dipendenti.

### 2.0 Aggiornamento della compliance privacy

Uno dei primari obiettivi del legislatore Europeo in fase di elaborazione del Regolamento UE 2016/679 è stato quello di garantire alle persone fisiche il controllo dei propri dati personali, la certezza giuridica e operativa, fosse rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche.
Tale principio pone il dovere in capo ad ogni Ente di aggiornare i propri sistemi in tema di trattamento dei dati al fine di adeguarsi a quanto richiesto dal legislatore Europeo stesso, attuando tutti gli strumenti necessari per rendere consapevole il cittadino di come vengono trattati i suoi dati personali.
Si è reso pertanto necessario procedere all'adeguamento dell'azienda con al Regolamento UE 2016/679 in tema di protezione dei dati personali sin dall'applicazione del Regolamento (maggio 2018).
La società si è quindi dotata di informative, incarichi, nomine per i responsabili del trattamento, ha dato corso ad una Valutazione di Impatto in relazione al trattamento dati conseguente l'installazione di un sistema di videosorveglianza, ed ha adottato un registro dei trattamenti.
La società ha altresì nominato un Responsabile della protezione dei dati.
In seguito, nel 2024, l'azienda ha dato corso ad una Valutazione di Impatto in relazione al trattamento dati conseguente l'implementazione di un canale interno di gestione delle segnalazioni *ex* D.Lgs. 24/2023.
Quindi, sempre nel 2024, la società, in una all'aggiornamento del Modello Organizzativo *ex* D.Lgs. 231/2001, si è determinata ad adottare il presente Codice di autoregolamentazione.
L'azienda si propone comunque di aggiornare tempestivamente la documentazione privacy pertinente, secondo il seguente calendario:

| | |
|---|---|
| Registro dei trattamenti | Aggiornamento annuale |
| Valutazioni di impatto | Aggiornamento ogni 12/18 mesi |
| Modelli di Informative, Nomine, Incarichi | Aggiornamento ogni 24 mesi |
| Codice di autoregolamentazione | Aggiornamento ogni 24 mesi |

In ogni caso sarà dato corso ad aggiornamenti al di fuori del calendario indicato nel caso di necessità (es. innovazioni significative nel flusso di dati interessato dal trattamento, che potrebbero impattare sui modelli e/o documenti adottati).

## 3.0 Finalità della compliance privacy

La compliance privacy deve essere informata ad attività di valutazione del rischio e finalizzata al miglioramento dei processi.
L'attività di compliance si propone come finalità quelle di:

- predisporre un sistema strutturato ed organico di procedure ed attività di controllo che abbia come obiettivo la riduzione del rischio di commissione di violazioni al trattamento dei dati mediante l'individuazione dei processi sensibili e la loro conseguente proceduralizzazione;
- creare, in tutti coloro che operano con, in nome, per conto e nell'interesse della azienda nelle aree di attività a rischio, la consapevolezza di poter incorrere – in caso di comportamenti non conformi alle prescrizioni del presente Codice nonché delle ulteriori norme e procedure aziendali, oltre che alla legge – in un illecito passibile di sanzioni, sul piano penale e amministrativo, irrogabili nei confronti della azienda stessa;

- garantire alla azienda, grazie a un'azione di controllo delle attività aziendali nelle aree di attività a rischio, la concreta ed effettiva possibilità di intervenire tempestivamente per prevenire la commissione di violazioni al corretto trattamento dei dati ovvero, individuare tempestivamente eventuali violazioni dei sistemi informatici della Società che possano esporre a rischi anche i dati trattati con i sistemi informatici stessi.

Il modello di compliance deve proporsi, altresì, di:

- sensibilizzare e diffondere a tutti i livelli aziendali le regole di condotta ed i protocolli per la programmazione della formazione e dell'attuazione delle decisioni della azienda, al fine di gestire e conseguentemente evitare il rischio della commissione di illeciti durante il trattamento dei dati, pertanto si incentivano le valutazioni d'impatto nonché l'applicazione dei principi di *privacy by design* e *privacy by default* come ampiamente descritti anche nel presente Codice di autoregolamentazione;
- individuare preventivamente le aree di attività a rischio afferenti l'attività della azienda, vale a dire le aree aziendali che risultano interessate dalle possibili casistiche di violazioni in ambito di trattamento dei dati ai sensi del Regolamento UE 2016/679;
- registrare correttamente le operazioni della azienda nell'ambito delle attività maggiormente esposte al rischio di illeciti durante il trattamento dei dati come previsti ai sensi del Regolamento UE 2016/679, ciò al fine di rendere possibile la verifica dei processi attuati durante il trattamento in seno alla azienda titolare del trattamento rintracciandone, di conseguenza, tutte i loro componenti rilevanti;
- valutare l'attività di tutti i soggetti che interagiscono con la azienda, sia nell'ambito dei trattamenti di maggior rischio, sia nell'ambito dei trattamenti che, per tipologia di dati trattati e finalità, espone la azienda stessa a minori rischi, curandone il necessario aggiornamento in relazione soprattutto alle novità normative che saranno introdotte.

## 4.0 I ruoli assunti da Azienda Trasporti Funicolari Malcesine Monte Baldo nel trattamento dei dati

Il ruolo concretamente assunto dall'azienda nel trattamento dei dati è principalmente quello di:

a. **Titolare del trattamento:** tale ruolo è assunto nello specifico in relazione ai dati trattati dei propri dipendenti, collaboratori, fornitori e clienti. Infatti, in relazione a tale trattamento la Società si occupa sia di raccogliere i dati presso gli interessati sia di gestire gli stessi in autonomia individuando le finalità e le modalità concrete di gestione degli stessi.

Non è comunque possibile escludere che l'azienda svolga altri ruoli ai sensi della normativa privacy, ad esempio**:**

b. **Contitolare del trattamento:** tale ruolo può essere assunto dall'azienda, ad esempio, in seno ad attività congiunte in sede di sponsorizzazione di eventi, attività;
c. **Responsabile del trattamento:** tale ruolo può essere assunto dall'azienda, ad esempio, qualora la stessa offra servizi ad aziende o amministrazioni (es. mettendo a disposizione sale convegni con attività di registrazione presenze o comunque di "segretariato" annesse).

## 5.0 Gli adempimenti del titolare

L'Azienda Trasporti Funicolari Malcesine Monte Baldo è un'azienda speciale regolata in larga parte dal diritto civile ed istituita per soddisfare prevalentemente bisogni di carattere commerciale (servizio di trasporto persone di tipo turistico).

Per definire gli adempimenti cui la stessa è tenuta dal punto di vista della normativa in materia di protezione dei dati personali è opportuno chiarire se la stessa possa considerarsi, a mente della normativa di riferimento, un'"autorità pubblica" o "un organismo pubblico".

Va premesso che la normativa GDPR non definisce autorità pubblica o organismo pubblico.

Per dare indicazioni in merito è intervenuto il Gruppo che raccoglie i Garanti europei (EDPB), il quale nelle sue linee guida (Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies) dice semplicemente che per la delimitazione delle categorie "autorità pubblica" e "organismo pubblico" occorre far riferimento al diritto nazionale.

Il diritto italiano non possiede però una definizione univoca di autorità pubblica e/o di organismo pubblico.

Il Gruppo europeo propone alcuni esempi di "organismo pubblico", sulla base della direttiva 2003/98/CE, relativa al riutilizzo dell'informazione del settore pubblico, e così include nella definizione gli enti:

- istituiti per soddisfare specificatamente bisogni d'interesse generale aventi carattere non industriale o commerciale, quantomeno in via prevalente;
- dotati di personalità giuridica;
- che presentino, inoltre, almeno uno dei seguenti tratti sintomatici: il finanziamento dell'attività, la soggezione al controllo di gestione, oppure la designazione di più della metà dei componenti degli organi di amministrazione, di direzione o di vigilanza da parte dello Stato, di enti pubblici territoriali o di altri organismi di diritto pubblico.

Parzialmente contrastante con questa lettura è quanto afferma il Garante nazionale, nelle sue FAQ sul DPO in ambito pubblico, dove è riportato: "*nel caso in cui soggetti privati esercitino funzioni pubbliche (in qualità, ad esempio, di concessionari di servizi pubblici), può risultare comunque fortemente raccomandato, ancorché non obbligatorio, procedere alla designazione di un DPO*".

Il Gruppo europeo è tornato in argomento affermando che ci sono alcuni ambiti in cui "*è verosimile che sia necessaria l'ulteriore tutela offerta dalla nomina di un DPO*", come: i trasporti pubblici, le forniture idriche ed elettriche, le infrastrutture stradali, le emittenti radiotelevisive pubbliche, gli istituti per l'edilizia pubblica o gli organismi di disciplina professionale.

In tutte queste ipotesi, in considerazione delle funzioni svolte e delle potestà esercitate, l'ente, quand'anche vestito di forma privatistica, assume una posizione di supremazia rispetto all'interessato, che lascia a quest'ultimo un esiguo margine di decisione circa il trattamento dei propri dati.

Calando queste considerazioni nel "contesto" dell'azienda, osserviamo come l'ente possieda con certezza due delle tre caratteristiche che "inquadrano" un ente come organismo pubblico, ovvero il controllo da parte di enti/organismi pubblici e la personalità giuridica.

Più complesso è definire se l'azienda è "istituita" per soddisfare prevalentemente bisogni d'interesse generale aventi carattere non industriale o commerciale.

Di fatto la risposta sembra negativa: l'Azienda Trasporti Funicolari è istituita per soddisfare prevalentemente bisogni di carattere commerciale (servizio di trasporto persone di tipo turistico), mentre solo in modesta parte potrebbe essere ricondotta al c.d. "servizio pubblico".

Vista però la presenza di alcuni indicatori (due su tre) che avvicinano l'azienda all'"organismo di diritto pubblico" come definito in sede europea, nonché viste le disposizioni statutarie che fanno ad oggi riferimento al "servizio pubblico" svolto dall'azienda, nel presente codice verrà adottata una posizione prudenziale, considerando applicabili le disposizioni del Reg. UE 2016/679 e della connessa normativa nazionale rivolte agli organismi di diritto pubblico, qualora più gravose.

Gli adempimenti cui è tenuta l'azienda sono, pertanto, i seguenti:

- adozione del registro dei trattamenti;
- valutazione d'impatto sulla protezione dei dati per quei trattamenti che coinvolgono un gran numero di dati e vengono svolti tramite sistemi informatici;
- adozione del responsabile per la protezione dei dati personali;
- informativa dettagliata ai cittadini di cui si trattano e detengono i dati;
- predisporre le nomine per i responsabili del trattamento nonché fornire istruzioni agli incaricati.

La struttura della compliance privacy aziendale si compone come segue:


## 5.1 Responsabile per la protezione dei dati

L'azienda ha proceduto a nominare il responsabile della protezione dei dati personali, che assume i seguenti compiti:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento UE 679/2016 nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b) sorvegliare l'osservanza del Regolamento UE 679/2016, di altre disposizioni dell'Unione o nazionali relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 Regolamento UE 679/2016;
d) cooperare con l'autorità di controllo; e
e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 Regolamento UE 679/2016, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

## 5.2 Amministratore di sistema

L'azienda ha proceduto a nominare i propri Amministratori di sistema, in esito ad una valutazione delle caratteristiche soggettive degli stessi (in termini di esperienza, capacità ed affidabilità), e ne conserva l'elenco in una apposita sezione del registro dei trattamenti.

L'Amministratore di sistema assume, ai sensi delle "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" adottate dal Garante privacy in data 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008), come modificate dal Provvedimento del 25.06.2009, i seguenti compiti:

- classificare analiticamente le banche dati e impostare un sistema complessivo di trattamento dei dati personali, predisponendo e curando ogni relativa fase applicativa nel rispetto della normativa vigente in materia di protezione dei dati personali;
- individuare per iscritto i soggetti incaricati della custodia delle parole chiave per l'accesso al sistema informativo e vigilare sulla loro attività;
- individuare per iscritto gli altri soggetti che possono avere accesso a informazioni che concernono le medesime;
- impostare e gestire un sistema di autenticazione informatica per i trattamenti di dati personali effettuati con strumenti elettronici;
- impostare e gestire un sistema di autorizzazione per gli incaricati dei trattamenti di dati personali effettuati con strumenti elettronici (sulla base del principio del privilegio minimo);
- adottare un sistema idoneo alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici; le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità, adeguate al raggiungimento dello scopo di verifica per cui sono richieste. Tali registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate ed essere conservate per un congruo periodo;
- assicurare e gestire sistemi di salvataggio e di ripristino dei dati (backup/recovery) anche automatici, nonché approntare adeguate misure e/o sistemi software di salvaguardia per la protezione dei dati personali (antivirus, firewall, IDS ecc.);
- impartire a tutti gli incaricati istruzioni organizzative e tecniche che prevedano le modalità di utilizzo dei sistemi di salvataggio dei dati con frequenza almeno settimanale;
- adottare procedure per la custodia delle copie di backup dei dati e per il ripristino della disponibilità dei dati e dei sistemi;
- organizzare i flussi di rete, la gestione dei supporti di memorizzazione, la manutenzione hardware, nonché la verifica di eventuali tentativi di accessi non autorizzati al sistema provenienti da soggetti terzi, quali accesso abusivo al sistema informatico o telematico, frode, danneggiamento di informazioni, dati e programmi informatici, danneggiamento di sistemi informatici e telematici;
- predisporre un piano di controlli periodici, da eseguire con cadenza almeno semestrale, atti a verificare l'efficacia delle misure di sicurezza adottate nell'azienda;

- coadiuvare, se richiesto, il titolare del trattamento nella predisposizione e/o nell'aggiornamento di tutti i documenti necessari per il rispetto del Reg. UE 2016/679.

L'Amministratore inoltre deve curare che gli accessi che lo stesso effettua sul sistema siano presidiati da sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

L'azienda dà corso ad un'attività di verifica annuale dell'operato degli Amministratori di sistema individuati, in modo da controllare la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.

## 5.3 Responsabile del trattamento

L'azienda è tenuta a nominare quale responsabile del trattamento ogni fornitore cui la stessa affidi un flusso di dati che quest'ultimo è tenuto a gestire per conto dell'azienda stessa.
Stando al disposto del Reg. UE 2016/679, il responsabile è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organo che tratta dati personali per conto del titolare del trattamento. Due condizioni sono indispensabili per configurare il ruolo di responsabile del trattamento: essere un soggetto distinto rispetto al titolare del trattamento e trattare dati personali per conto del titolare del trattamento.
Al responsabile del trattamento non è consentito trattare i dati in modo diverso rispetto a quanto indicato nelle istruzioni del titolare. Tuttavia, le istruzioni del titolare del trattamento possono lasciare un certo margine di discrezionalità su come servirne al meglio gli interessi, consentendo al responsabile del trattamento di avvalersi dei mezzi tecnici e organizzativi più idonei. Ciononostante, un responsabile del trattamento viola il GDPR qualora non si limiti a trattare i dati in base alle istruzioni del titolare del trattamento e inizi a definire mezzi e finalità propri. Il responsabile del trattamento sarà pertanto considerato titolare rispetto a tale ultimo trattamento e può essere soggetto a sanzioni qualora non si limiti a trattare i dati in base alle istruzioni impartite dal titolare del trattamento.

Sul punto, le pertinenti linee guida EDPB (Guidelines 07/2020 on the concepts of controller and processor in the GDPR) precisano che:

Le due condizioni fondamentali per la qualifica di responsabile del trattamento sono:

a) essere un soggetto distinto rispetto al titolare del trattamento;
b) trattare i dati personali per conto del titolare del trattamento.

Un soggetto distinto significa che il titolare del trattamento decide di delegare tutte o parte delle attività di trattamento a un soggetto esterno. All'interno di un gruppo di società, una di esse può essere responsabile del trattamento di un'altra che

agisce in qualità di titolare del trattamento, in quanto le due società sono entità distinte. Di converso, un dipartimento all'interno di una società non può essere responsabile del trattamento per conto di un altro dipartimento all'interno della stessa società.
Se il titolare del trattamento decide di trattare direttamente i dati utilizzando le proprie risorse interne, ad esempio attraverso il proprio personale, non vi sono responsabili del trattamento. I dipendenti e le altre persone che agiscono sotto l'autorità diretta del titolare del trattamento, come il personale assunto temporaneamente, non vanno considerati responsabili del trattamento poiché trattano dati personali in quanto parte della struttura del titolare del trattamento. Conformemente all'articolo 29 Reg. UE 2016/679, essi sono altresì vincolati dalle istruzioni del suddetto titolare.
Il trattamento di dati personali per conto del titolare comporta innanzitutto che il soggetto distinto tratti i dati personali a beneficio del titolare del trattamento. All'articolo 4, paragrafo 2 Reg. UE 2016/679, per trattamento si intende un'ampia gamma di operazioni, dalla raccolta alla conservazione, dalla consultazione all'uso, dalla diffusione o qualsiasi altra forma di messa a disposizione fino alla distruzione.
In secondo luogo, il trattamento deve essere effettuato per conto di un titolare, ma non agendo sotto la sua autorità o controllo diretti. Agire «per conto di» significa servire gli interessi di terzi e richiama la nozione giuridica di «delega». Nel caso della normativa in materia di protezione dei dati, il responsabile del trattamento è chiamato a seguire le istruzioni impartite dal titolare almeno per quanto concerne la finalità del trattamento e gli elementi essenziali che ne costituiscono i mezzi. La liceità del trattamento, ai sensi dell'articolo 6 e, se pertinente, dell'articolo 9 del Reg. UE 2016/679, deriva dall'attività del titolare del trattamento: il responsabile del trattamento non deve trattare i dati in modo diverso da quanto indicato nelle istruzioni del suddetto titolare. Tuttavia, come detto in precedenza, le istruzioni del titolare del trattamento possono lasciare un certo margine di discrezionalità su come servire al meglio i suoi interessi; ciò consente al responsabile del trattamento di scegliere i mezzi tecnici e organizzativi più idonei.
Agire «per conto di» significa inoltre che il responsabile del trattamento non può effettuare trattamenti per finalità proprie. Ai sensi dell'articolo 28, paragrafo 10, il responsabile del trattamento è in violazione del GDPR qualora non si limiti a trattare i dati in base alle istruzioni del titolare del trattamento e inizi a definire proprie finalità e propri mezzi di trattamento. Il responsabile del trattamento si configura come titolare in un caso del genere e può essere soggetto a sanzioni qualora non si limiti a trattare i dati in base alle istruzioni del titolare.

## 5.4 Registro dei trattamenti

L'azienda ha adottato un registro dei trattamenti svolti dalla stessa.
Il registro dei trattamenti dovrà essere aggiornato ogni volta che verrà introdotto un nuovo trattamento ovvero sarà modificato, anche solo in parte, una tipologia di trattamento oggi adottato.
Il registro così compilato sarà messo a disposizione degli interessati che ne facciano formale richiesta ovvero all'Autorità di controllo in caso di verifiche o segnalazioni che vedano coinvolta l'azienda.
Il registro (così come i suoi aggiornamenti) deve essere formalmente adottato dalla Direzione generale con registrazione di protocollo o altro strumento idoneo a garantirne la datacertazione.

## 5.5 Valutazione di impatto

Come previsto dal Regolamento UE 2016/679 al considerando n. 84, per potenziare il rispetto al Regolamento stesso, qualora i trattamenti possano prestare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento dovrebbe essere responsabile dello svolgimento della valutazione d'impatto sulla protezione dei dati per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio.
L'esito delle valutazioni dovrebbe essere preso in considerazione nella determinazione delle opportune misure da adottare per garantire la sicurezza dei trattamenti che vengono attuati.
In conformità a quanto richiesto dal Regolamento UE 2016/69 l'azienda ha individuato quei trattamenti che o per tipologia di dati trattati o per strumenti utilizzati necessitassero di una valutazione d'impatto e vi ha dato corso.
Per i trattamenti individuati si è quindi provveduto a contattare i fornitori dei sistemi informatici stessi al fine di vagliare e monitorare le misure di sicurezza attualmente in uso e, ove si fosse ritenuto necessario, prevedere delle possibili modifiche e/o implementazioni delle stesse al fine di garantire un maggior livello di sicurezza del trattamento in conformità e nel rispetto di quanto previsto dal Regolamento UE stesso.
I risultati delle valutazioni sono stati riportati in apposito documento e richiamate nel registro dei trattamenti.
Nel dettaglio sono state svolte le seguenti valutazioni di impatto:

- in relazione al trattamento svolto nei confronti dei dipendenti della Società, di clienti e fornitori, nonché dei terzi che accedono alla sede aziendale, in relazione al sistema di videosorveglianza installato;
- in relazione al trattamento derivante dall'implementazione di un canale informatico per gestire le segnalazioni di cui al D.Lgs. 24/2023 (Whistleblowing).

## 5.6 Redazione delle informative rivolte agli interessati

Il Regolamento UE 2016/679 ha imposto a tutti i titolari del trattamento e a tutti i responsabili del trattamento di fornire un'informativa dettagliata all'interessato in relazione alla tipologia di dati che vengono raccolti, quali sono le finalità per le quali i dati sono stati raccolti, la durata del trattamento e, infine, anche quali sono le modalità, a disposizione dell'interessato stesso, per proporre reclamo, ricorso ovvero accedere ai suoi dati in presso il titolare del trattamento.

L'azienda ha quindi predisposto una serie di informative rivolte alle diverse tipologie di trattamenti effettuati, nello specifico:

Informativa Fornitori (T1)

Consenso Fornitori (C1)

Informativa Clienti (T2)
"abbonamento invernale"

Informativa Curriculum (T4)

Informativa Candidati Bandi (T5)

Informativa Videosorveglianza – ITA
Informativa Videosorveglianza – ENG

Informativa dipendenti

## POLICY AZIENDALI

### A - Documentazione circa la sottoposizione delle informative e la raccolta dei consensi

In occasione del primo accesso dell'utente presso l'azienda, sia essa presso la sede o tramite contatto con modalità telematiche, è necessario verificare che sia stata allo stesso sottoposta l'informativa in relazione al trattamento di dati personali.

Nel caso di sottoposizione dell'informativa in modalità cartacea è necessario documentare che la stessa sia stata effettivamente sottoposta all'interessato e ciò è possibile in diversi modi:

- acquisendo la sottoscrizione dell'interessato;
- acquisendo la sottoscrizione dell'interessato in relazione ad un separato documento (es. contratto di fornitura) di cui l'informativa costituisca allegato;
- documentando compiutamente il processo per cui l'informativa è sottoposta attraverso modalità ulteriori (es. presenza dell'informativa sul retro del biglietto di ingresso, o presso i locali), in questi casi è necessario documentare compiutamente (con relazioni e se del caso immagini) il momento in cui l'informativa ha iniziato ad essere sottoposta con tale modalità, nonché il momento in cui sono state implementate modifiche o aggiornamenti alla documentazione e/o al processo di sottoposizione (va precisato che queste modalità non sono idonee a raccogliere il consenso dell'interessato).

Nel caso di sottoposizione dell'informativa in modalità informatica è necessario documentare che la stessa sia stata effettivamente sottoposta all'interessato e ciò è possibile in diversi modi:

- inviando via mail l'informativa all'interessato;
- acquisendo una sottoscrizione con firma elettronica sul documento;
- ottenendo un flag su modulo informatico (in tale caso è però essenziale documentare a livello informatico e senza possibilità di alterazione il processo che ha condotto all'acquisizione del flag e la sua connessione con lo specifico testo di informativa sottoposto, ad esempio affidandosi ad un fornitore certificato che non consente la modifica dei moduli sottoposti e dei relativi allegati oppure documentando lo stato del modulo su siti terzi ed affidabili, es. Wayback Machine).

In entrambi i casi l'informativa, insieme alla documentazione fisica o informatica che ne attesta la sottoposizione all'interessato, deve essere conservata per tutta la durata del trattamento (è importante tenere quindi presente che nel caso ci si affidi ad un fornitore terzo per la conservazione della documentazione di processo relativa alla sottoposizione dell'informativa, andrà valutato con attenzione il processo con cui il fornitore stesso consente di estrarre i dati relativi, perché nel caso con questo trasferimento si verifichi una perdita di conoscenza (es. possibile alterazione di lì in avanti del dato) è necessario mantenere il rapporto con il fornitore fino all'esaurimento del trattamento ed alla compiuta cancellazione dei dati personali cui l'informativa si riferisce.

I processi di sottoposizione delle informative devono quindi essere predisposti dal Referente privacy aziendale e se del caso approvati dalla Direzione generale.

## B – Richieste di accesso

**1. Introduzione**

1.1 Il Titolare detiene dati personali (o informazioni) sui propri dipendenti, fornitori e clienti.

1.2 Ai sensi del regolamento (UE) 2016/679, Regolamento generale sulla protezione dei dati (GDPR), le persone fisiche (c.d. "**persone interessate**") hanno il diritto generale di conoscere se conserviamo o trattiamo dati su di loro, le modalità di accesso a tali dati, nonché eventuali informazioni ulteriori.

1.3 Questa policy fornisce una guida ad uso interno in merito alla gestione delle richieste di accesso ai dati personali da parte degli interessati. Non è una policy sulla privacy e non deve essere trasmessa a terze parti.

1.4 Questa policy si applica a tutto il personale e non solo al soggetto delegato dal Titolare alla risposta alle istanze di accesso ("**referente privacy**").

In particolare, questa policy fornisce indicazioni su:

- cosa fare se si riceve una richiesta di accesso ai propri dati personali da parte degli interessati; e
- come individuare una richiesta di accesso ai dati da parte dell'interessato.

1.5 Il Titolare esaminerà e aggiornerà regolarmente questa policy in conformità con gli obblighi di protezione dei dati. Non facendo parte tale attività del contratto di lavoro del personale dipendente tale documento potrà essere modificato, aggiornato, completato e comunicato di volta in volta.

1.6 In caso di domande relative a questo documento si prega di contattare il Referente privacy(raggiungibile all'indirizzo email privacy@funiviedelbaldo.it "**Referente privacy**").

**2 Come riconoscere una richiesta di accesso dell'interessato**

**(istruzioni rivolte a: <u>tutto il personale</u>)**

2.1 Una richiesta di accesso dell'interessato è una richiesta di un individuo (o di qualcuno che agisce per suo conto, ad esempio un genitore che fa una richiesta in relazione alle informazioni relative al proprio figlio):

- per la conferma del trattamento dei dati personali su di lui o lei;
- per l'accesso a tali dati personali;
- e alcune altre informazioni supplementari.

2.2 Tale richiesta sarà tipicamente redatta per iscritto (nelle policy elaborate dal Titolare è indicato che la richiesta deve essere effettuata per email all'indirizzo privacy@funiviedelbaldo.it o a mezzo raccomandata o PEC) ma può essere effettuata anche con altre modalità e infine anche oralmente (ad esempio durante una conversazione telefonica). La richiesta può fare riferimento al GDPR e/o alla "**protezione dei dati**" e/o ai "**dati personali**", ma non è un requisito necessario affinché la richiesta sia considerata valida. Ad esempio, una lettera che recita "*per favore fornitemi una copia di tutte le informazioni che avete su di me*" sarà una richiesta di accesso per l'interessato e dovrebbe essere trattata come tale.
2.3 Tutte le richieste di accesso ai dati devono essere immediatamente indirizzate al Referente privacy dal Titolare per rispondere alle richieste (raggiungibile all'indirizzo email privacy@funiviedelbaldo.it).

**3 Cosa fare quando si riceve una richiesta di accesso ai dati da parte dell'interessato**
**(istruzioni rivolte a: tutto il personale)**
3.1 Ogniqualvolta si riceve una richiesta di accesso da parte dell'interessato e non si è autorizzati alla relativa gestione, è necessario adottare immediatamente le misure di cui ai paragrafi 3.3 (richiesta ricevuta via e-mail) o 3.4 (richiesta ricevuta per lettera) al fine di evitare qualsiasi ritardo nel fornire riscontro.
3.2 Se non si è certi che una richiesta di informazioni sia una richiesta di accesso da parte dell'interessato, si prega di confrontarsi con il Referente privacy (raggiungibile all'indirizzo email privacy@funiviedelbaldo.it).
3.3 Se si riceve una richiesta di accesso dell'interessato via e-mail, è necessario inoltrare immediatamente la richiesta al Referente privacy a mezzo email a questo indirizzo di posta elettronica: privacy@funiviedelbaldo.it
3.4 Se si riceve una richiesta di accesso per oggetto dei dati per lettera, è necessario:

- scansionare la lettera;
- consegnare l'originale al Referente privacy dal Titolare per rispondere alle richieste;
- inviare una copia scannerizzata della lettera a questo indirizzo email: privacy@funiviedelbaldo.it

3.5 Se si riceve oralmente una richiesta di accesso per l'oggetto dei dati, è necessario:

- prendere nota del nome e dei dettagli di contatto del richiedente;
- informare il richiedente che comunicherà al soggetto incaricato la sua richiesta e che verrà contattato in relazione alla stessa;
- inviare immediatamente un'email al Referente privacy a questo indirizzo di posta elettronica: privacy@funiviedelbaldo.it fornendo i dettagli di contatto dell'individuo e i dettagli della richiesta orale e la data in cui è stata ricevuta.

3.6 Il Referente privacy dovrà sempre inviare una conferma di avvenuta ricezione della comunicazione. Se non si riceve tale conferma entro due giorni lavorativi dall'invio, è necessario contattare il Referente privacy per confermare la ricezione.
3.7 Non si devono intraprendere altre azioni in relazione alla richiesta di accesso dell'interessato, salvo su richiesta da parte del Referente privacy dal Titolare per rispondere alle richieste.

**4 Condizioni per rispondere a una richiesta valida**
**(istruzioni rivolte a: Referente privacy)**
4.1 Laddove il Titolare tratti una grande quantità di informazioni riferibili allo stesso soggetto (es. un dipendente), potrebbe essere necessario chiedere allo stesso di specificare le informazioni o le attività di elaborazione a cui si riferisce la richiesta.

4.2 Il Titolare non addebita una commissione per rispondere a una richiesta di accesso ai dati da parte dell'interessato. Tuttavia, il Titolare si riserva di addebitare un costo per rispondere a una richiesta di accesso ai dati personali nel caso in cui:

- la stessa risulti manifestamente infondata, eccessiva, ultronea (es. richiesta ripetitiva);
- vengono richieste più copie delle stesse informazioni.

Nel caso, il Referente privacy, al fine di quantificare l'addebito, dovrà previamente confrontarsi con la Direzione generale.

**5 Identificazione dell'interessato**
**(istruzioni rivolte a: Referente privacy)**

5.1 Prima di rispondere a una richiesta di accesso ai dati personali da parte dell'interessato, è necessario adottare idonee misure per verificare l'identità della persona che effettua la richiesta. In genere richiederemo una copia di un documento di identità in corso di validità del richiedente.

5.2 In caso di dubbi sull'identità della persona che effettua la richiesta di accesso ai dati personali, potremmo chiedere ulteriori informazioni per avere conferma circa la sua identità (es. richiesta formulata per iscritto e sottoscritta dall'interessato, copia sottoscritta del documento di identità, ..).

5.3 Se non saremo in grado di identificare l'interessato, nonostante siano state richieste ulteriori informazioni, potremmo rifiutare di evadere la relativa richiesta di accesso ai dati personali da parte dell'interessato.

5.4 In caso di delega a terzi a richiedere le informazioni, i terzi dovranno fornire idonea delega da parte dell'interessato unitamente a copia del documento identità del delegante e del delegato.

**6 Rifiuto di rispondere a una richiesta**
**(istruzioni rivolte a: Referente privacy)**

6.1 Si dovrà rifiutare di rispondere ad una richiesta di accesso ai dati personali da parte dell'interessato quando:

- anche dopo aver richiesto informazioni aggiuntive in conformità al paragrafo 5.2, non si è in grado di identificare l'individuo che ha effettuato la richiesta di accesso;
- le richieste dell'interessato sono manifestamente infondate, eccessive, ultronee o generiche.

6.2 In detti casi si dovrà comunicare all'interessato il rifiuto di evadere la richiesta di accesso ai dati personale non oltre un mese dopo aver ricevuto la relativa richiesta, con indicazione:

- dei motivi per cui si è provveduto in tal senso;
- della possibilità in capo all'interessato di sporgere reclamo avanti il Garante per la protezione dei dati personali ovvero degli eventuali rimedi giudiziari a disposizione.

**7 Termine per rispondere a una richiesta**
**(istruzioni rivolte a: Referente privacy)**

7.1 Una volta ricevuta una richiesta di accesso ai dati da parte dell'interessato, il Titolare dovrà fornire le informazioni richieste senza indugio e al più tardi entro un mese dal ricevimento della richiesta. Si deve quindi prendere nota di quando è stata ricevuta la richiesta e di quando della scadenza del predetto termine.

7.2 Se una richiesta di accesso ai dati personali è complessa o l'interessato ha fatto numerose richieste, il Titolare potrà prorogare tale periodo (avendo cura di non superare i tre mesi dalla data della richiesta), informando entro un mese dalla richiesta della proroga, indicandone i motivi.

**8 Informazioni da fornire in risposta a una richiesta di accesso ai dati personali**
**(istruzioni rivolte a: Referente privacy)**

8.1 L'interessato ha diritto a ricevere i dati personali trattati su di lui o lei e le seguenti informazioni:

- le finalità per le quali il Titolare tratta i dati personali;
- i destinatari o le categorie di destinatari a cui sono stati o saranno comunicati i dati personali, in particolare se tali destinatari si trovano in paesi terzi o organizzazioni internazionali;
- ove possibile, il periodo per il quale è previsto che i dati personali saranno archiviati, o, se non possibile, i criteri utilizzati per determinare tale periodo;
- il fatto che l'individuo abbia il diritto di:

(a) richiedere che il Titolare rettifichi, cancelli o limiti il trattamento dei propri dati personali; o
(b) di opporsi al trattamento;
(c) presentare un reclamo al Garante per la protezione dei dati personali;

- se i dati personali non sono stati raccolti presso l'interessato (es. dati di soggetti messi a disposizione da un fornitore), qualsiasi informazione disponibile riguardo alle fonti dei dati personali;
- qualsiasi decisione automatizzata che il Titolare avesse preso su di lui o lei (si fa presente che ad oggi il Titolare non assume decisioni automatizzate circa i soggetti di cui tratta i dati), insieme a informazioni significative sulla logica utilizzata, nonché sul significato e gli effetti conseguenti di tale elaborazione per lui o lei).

8.2 Le informazioni di cui al paragrafo 8.1 devono essere fornite:

- in modo conciso, trasparente, di facile comprensione e di facile accesso;
- utilizzando un linguaggio chiaro e semplice, con qualsiasi termine tecnico o abbreviazione;
- per iscritto, se la richiesta di accesso dell'interessato è stata fatta per iscritto;
- in un formato elettronico di uso comune, se la richiesta di accesso alla persona interessata è stata effettuata elettronicamente, se non diversamente richiesto dall'interessato; e
- ove possibile, fornendo l'accesso remoto a un sistema sicuro che fornisca all'interessato l'accesso diretto ai suoi dati personali.

**9 Processo decisionale automatizzato**
**(istruzioni rivolte a: Referente privacy)**
**Si segnala che ad oggi il Titolare non assume decisioni in forma automatizzata**

9.1 Se la richiesta di accesso ai dati personali dell'interessato al trattamento richiede specificamente informazioni sulla logica alla base di qualsiasi decisione automatica che abbiamo preso in relazione a questioni importanti relative alla persona (es. rendimento sul lavoro, merito di credito, affidabilità o condotta), il Titolare dovrà fornire una descrizione della logica implicita in tale decisione automatizzata, alle seguenti condizioni:

- la decisione automatizzata deve aver costituito l'unica base per la decisione, senza che vi sia stato alcun intervento umano;
- nel fornire una descrizione della logica non siamo tenuti a rivelare alcuna informazione che costituisce un segreto commerciale.

9.2 Se il Titolare effettua un processo decisionale automatizzato in relazione a una persona, la richiesta di accesso ai dati personali da parte dell'interessato può includere una richiesta:

- di informazioni relative alla decisione automatizzata;
- di intervento umano da parte del Titolare, vale a dire chiedere a una persona con il potere e le competenze per modificare la decisione di riesaminare la decisione automatizzata, considerando tutti i dati disponibili;
- di poter esprimere il proprio punto di vista sulla decisione automatizzata;
- di contestazione della decisione automatizzata.

Se tale richiesta viene ricevuta, il Referente privacy farà in modo che venga trattata in conformità al GDPR e alle altre normative e linee guida pertinenti.

**10 Come individuare le informazioni**
**(istruzioni rivolte a: Referente privacy)**

10.1 I dati personali che devono essere forniti in risposta a una richiesta di accesso ai dati personali da parte dell'interessato al trattamento possono trovarsi in diversi dei nostri sistemi di archiviazione elettronici e manuali. Questo è il motivo per cui è importante identificare sin dall'inizio il tipo di informazioni richieste affinché la ricerca possa essere puntuale.

10.2 A seconda del tipo di informazioni richieste, potrebbe essere necessario effettuare una ricerca:

- nei sistemi elettronici, ad es. database, computer in rete e non in rete, server, record dei dipendenti, dati di posta elettronica, dati di posta elettronica certificata, dati di backup, dati inseriti in gestionali in uso;
- nei sistemi di archiviazione manuali in cui i dati personali sono accessibili secondo criteri specifici, ad esempio insiemi ordinati cronologicamente di registrazioni manuali contenenti dati personali;
- nei sistemi di dati detenuti esternamente dai collaboratori esterni del Titolare, ad esempio fornitori di servizi di paghe esterni.

10.3 É necessario cercare in questi sistemi utilizzando il nome dell'individuo, nonché, a seconda dei casi, il numero del dipendente, il numero di pratica (ove individuato), ovvero altro identificativo dell'interessato.

**11 Selezione dei dati personali**
**(istruzioni rivolte a: Referente privacy)**

11.1 Una volta eseguita la ricerca e raccolti i risultati, sarà necessario selezionare le informazioni da fornire in risposta alla richiesta di accesso ai dati personali da parte dell'interessato. L'interessato ha il diritto di ricevere le informazioni che costituiscono i suoi dati personali.

11.2 Dati personali sono tutte le informazioni che permettono di identificare una persona fisica direttamente o indirettamente, in particolare facendo riferimento a un dato identificativo, ad esempio il loro nome, numero di identificazione, dati di localizzazione o identificativo online. Si possono ritenere inclusi nella nozione di dati personali anche le informazioni che sono state pseudonimizzate (ad esempio, codificati mediante chiave), a seconda della difficoltà ad attribuire lo pseudonimo a un particolare individuo.

11.3 I dati personali possono essere anche riportati in forma di elenco o modulo, ove del caso ed ove questo consenta una più efficiente gestione della richiesta.

**12 Deroghe al diritto di accesso dell'interessato**
**(istruzioni rivolte a: Referente privacy)**

12.1 In determinate circostanze potremmo essere esentati dal fornire alcuni o tutti i dati personali richiesti. Queste esenzioni sono descritte di seguito e dovrebbero essere applicate di volta in volta dopo un'attenta considerazione di tutti i fatti.

12.2 Rilevazione e prevenzione del crimine: non dobbiamo divulgare alcun dato personale che stiamo trattando al fine di prevenire o individuare un crimine; arrestare o perseguire i trasgressori. Questa non è un'esenzione assoluta. Si applica solo nella misura in cui l'accesso dell'interessato potrebbe pregiudicare uno di questi scopi. Ad esempio, se la divulgazione dei dati personali potrebbe allertare l'interessato sul fatto che lui o lei è indagato per un'attività illegale, allora non dobbiamo divulgare i dati poiché la divulgazione potrebbe pregiudicare la prevenzione o l'individuazione di reati o l'arresto o il perseguimento dei trasgressori.

12.3 Protezione dei diritti di terzi: non è necessario divulgare dati personali nella misura in cui ciò comporterebbe la divulgazione di informazioni relative a un altro individuo (comprese le informazioni che identificano un altro individuo come fonte di informazioni) che può essere identificato dalle informazioni (o che tali informazioni e ogni altra informazione che riteniamo idonea che l'interessato possa possedere o ottenere), a meno che:

- l'altra persona abbia acconsentito alla divulgazione delle informazioni al soggetto che ha fatto la richiesta; o
- è ragionevole divulgare le informazioni alla persona che presenta la richiesta senza il consenso dell'altro individuo, avendo riguardo a:

(a) il tipo di informazioni che sarebbero divulgate;
(b) qualsiasi obbligo di riservatezza nei confronti dell'altro soggetto;
(c) qualsiasi misura adottata al fine di ottenere il consenso dell'altro soggetto;
(d) se l'altro soggetto è in grado di dare il consenso; e
(e) qualsiasi rifiuto esplicito di consenso da parte dell'altro soggetto.

12.4 Raccomandazioni confidenziali: non è necessario divulgare le raccomandazioni confidenziali che abbiamo fornito a terzi per i seguenti fini effettivi o potenziali:

- istruzione, formazione o impiego dell'interessato;
- incarichi ricoperti dell'interessato.

Questa esenzione non si applica alle raccomandazioni confidenziali che riceviamo da terze parti. Tuttavia, in questa situazione, l'eventuale richiesta di accesso dell'interessato potrebbe comportare la rivelazione dei dati personali di un altro soggetto (ossia la persona che fornisce la raccomandazione), il che significa che sarà necessario considerare le regole relative alla divulgazione dei dati di terzi prima di divulgare la fonte.

12.5 Informazioni soggette al segreto professionale: non è necessario divulgare alcun dato personale soggetto al segreto professionale. Il segreto professionale riguarda qualsiasi documento che sia stato creato con lo scopo principale di essere utilizzato in qualsiasi forma di contenzioso. Una volta che termina il segreto professionale, i documenti diventano disponibili se viene ricevuta una richiesta di accesso dell'interessato.

Se si ritiene che l'esenzione per privilegi professionali legali possa applicarsi ai dati personali che sono stati richiesti, la questione va condivisa con la Direzione generale ed il DPO prima di assumere una decisione.

12.6 Finanziamenti aziendali: non è necessario divulgare alcun dato personale trattato ai fini di, o in relazione a, un servizio di finanza aziendale se:

- divulgare i dati personali potrebbe influire sul prezzo di uno strumento finanziario; o

- la divulgazione dei dati personali avrebbe un effetto pregiudizievole sul corretto funzionamento dei mercati finanziari o sull'allocazione efficiente del capitale all'interno dell'economia e riteniamo che potrebbe influenzare la decisione di una persona:

(a) se negoziare, sottoscrivere o emettere uno strumento finanziario;
(b) se agire in modo tale da avere un effetto su un'attività economica, ad esempio sulla strategia industriale di una persona, sulla struttura patrimoniale di un'impresa o sulla proprietà legale o beneficiaria di un'attività o di un'attività.
12.7 Previsioni di gestione: non è necessario divulgare alcun dato personale trattato ai fini di gestione o di pianificazione per aiutarci nello svolgimento di qualsiasi attività commerciale o di qualsiasi altra attività.
12.8 Negoziati: non è necessario divulgare alcun dato personale costituito da registrazioni delle intenzioni del Titolare in relazione a qualsiasi trattativa con l'interessato, in quanto ciò potrebbe pregiudicare tali negoziati.

**13 Eliminazione dei dati personali**
**(istruzioni rivolte a: Referente privacy)**
13.1 Le informazioni che ci vengono richieste attraverso una richiesta di accesso ai dati personali da parte dell'interessato dovranno essere fornite facendo riferimento ai dati personali trattati al momento della ricezione della richiesta. Tuttavia, poiché abbiamo un mese di tempo per rispondere e generalmente non riusciremo a rispondere nella stessa giornata in cui riceveremo la richiesta, siamo autorizzati a prendere in considerazione qualsiasi modifica o cancellazione da apportare ai dati personali tra il momento in cui la richiesta è ricevuta e il momento in cui i dati personali saranno forniti se tale modifica o cancellazione si sarebbe effettuata indipendentemente dalla ricezione della richiesta di accesso ai dati da parte dell'interessato.
13.2 Siamo pertanto autorizzati a svolgere attività di pulizia periodiche anche se ciò significa che cancelliamo o rettifichiamo i dati personali dopo la ricezione di una richiesta di accesso ai dati personali da parte dell'interessato. Quello che non possiamo fare è modificare o cancellare i dati per evitare di fornire gli stessi all'interessato.

**14 Conseguenze del mancato rispetto di questa policy**
**(istruzioni rivolte a: tutto il personale)**
14.1 Se non rispetteremo una richiesta di accesso ai dati personali da parte dell'interessato al trattamento, o non forniremo l'accesso a tutti i dati personali richiesti, o non risponderemo entro il termine di un mese, violeremo il GDPR. Questo potrebbe avere diverse conseguenze:

- potrebbe mettere a rischio la/le persona/e i cui dati personali vengono trattati;
- l'interessato potrebbe presentare un reclamo al Garante per la protezione dei dati personali e ciò potrebbe indurre il Garante per la protezione dei dati personali a istruire il reclamo. In caso di violazione, è possibile che venga intrapresa un'azione legale che potrebbe comportare il rischio di gravi sanzioni civili e penali per il Titolare e, in alcune circostanze, per il singolo responsabile della violazione;
- se una persona ha subito danni, o lesioni, a seguito della violazione del GDPR, il Titolare potrebbe essere citato in Tribunale; e
- un Tribunale potrebbe ordinare al Titolare di soddisfare la richiesta di accesso ai dati personali da parte dell'interessato se risulta che non siano stati rispettati gli obblighi previsti ai sensi del GDPR.

14.2 A causa dell'importanza di questa policy, la mancata osservanza da parte di un dipendente o collaboratore di qualsiasi sua parte potrebbe comportare un'azione disciplinare.

**15 Contatti e responsabilità**
**(istruzioni rivolte a: tutto il personale)**
15.1 La presente Policy sarà riesaminata ogni due anni dal Referente privacy del Titolare per la gestione delle richieste di accesso, insieme al soggetto responsabile del settore IT per quanto di sua competenza e salvo modifiche aziendali e/o esigenze che rendano necessario un intervento con tempistiche più ridotte.
15.2 Qualsiasi domanda riguardante questa policy dovrà essere indirizzata al Referente privacy (raggiungibile all'indirizzo email privacy@funiviedelbaldo.it) ovvero, in caso di residui dubbi, al DPO.
15.3 Ulteriori richieste di accesso (es. accesso civico) andranno trattate secondo i criteri di cui alla presente policy, in quanto compatibili, qualora le stesse coinvolgano dati personali.

## C – Data Breach

**1 Introduzione**
Una violazione dei dati personali trattati dal Titolare può comportare danni alle persone, alla reputazione, avere effetti dannosi sul nostro operato, comportare una non conformità a previsioni legislative e/o costi finanziari.

**2 Scopo**
2.1 Il Titolare è obbligato, ai sensi del Reg. UE 2016/679 (GDPR) a garantire la sicurezza di tutti i dati personali durante il loro trattamento.
2.2 La presente policy definisce la procedura da seguire per garantire un approccio coerente ed efficace per la gestione degli incidenti relativi alla violazione dei dati e alla sicurezza delle informazioni del Titolare.

**3 Obiettivo**
3.1 La presente policy si riferisce a tutti i dati personali, particolari e giudiziari detenuti dal Titolare indipendentemente dal loro formato. Per "**dato personale**" si considera 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 (art. 4 Reg. UE 2016/679).
3.2 Questa policy si applica a tutto il personale dipendente ed ai consulenti, i fornitori e i responsabili del trattamento dei dati che lavorano per o per conto del Titolare.
3.3 L'obiettivo di questa policy è contenere eventuali violazioni, minimizzare il rischio associato alla violazione e considerare quale azione è necessaria per proteggere i dati personali e prevenire ulteriori violazioni.

**4 Definizione/Tipi di violazione**
4.1 Ai fini della presente policy, le violazioni della sicurezza dei dati comprendono altresì le perdite di dati accidentali, confermate o sospette.

4.2 Un incidente nel contesto di questa policy è un evento o un'azione 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 dal Titolare, violazione che ha causato o può potenzialmente causare danni al patrimonio informativo e/o alla reputazione del Titolare o degli interessati.
4.3 Un incidente include ma non è limitato a quanto segue:

- perdita o furto di dati o apparecchiature riservate o sensibili su cui tali dati sono archiviati (ad esempio, perdita di laptop, chiavetta USB, dispositivo iPad / tablet o carta);
- furto o guasto dell'apparecchiatura;
- uso non autorizzato, accesso o modifica di dati o sistemi di informazione;
- tentativi (non riusciti o riusciti) di ottenere accesso non autorizzato alle informazioni o ai sistemi IT;
- divulgazione non autorizzata di dati sensibili / confidenziali;
- malfunzionamento del sito web;
- attacco hacker;
- situazioni impreviste come un incendio o un'inondazione;
- errore umano nella gestione del dato personale.

**5 Segnalazione di un incidente**

5.1 Chiunque acceda, utilizzi o gestisca le informazioni del Titolare è tenuto a segnalare immediatamente le violazioni alla sicurezza dei dati e gli incidenti informatici al Titolare o a Suo delegato (Referente privacy raggiungibile all'email privacy@funiviedelbaldo.it).
5.2 Se la violazione si verifica o viene scoperta al di fuori del normale orario di lavoro, deve essere segnalata non appena possibile e ne va fornito idoneo rapporto.
5.3 Il rapporto includerà i dettagli completi e accurati dell'incidente, quando si è verificata la violazione (data e ora), chi lo segnala, se i dati si riferiscono alle persone, la natura delle informazioni e il numero di persone coinvolte. Un modulo di segnalazione degli incidenti dovrebbe essere completato come parte del processo di segnalazione. Si veda **Allegato 1**
5.4 Tutto il personale e i collaboratori devono essere consapevoli che qualsiasi violazione della legge sulla protezione dei dati può comportare l'attivazione di procedure disciplinari.

**6 Contenimento e recupero**

6.1 Il Referente privacy determinerà in primo luogo se la violazione è ancora in corso. In tal caso, verranno presi immediatamente i provvedimenti appropriati per ridurre al minimo gli effetti della violazione.
6.2 Una valutazione iniziale sarà effettuata (se del caso unitamente all'Amministratore di Sistema nonché del responsabile e agli addetti del reparto IT) dal Referente privacy per stabilire la gravità della violazione e assumerà le iniziative necessarie per indagare sulla violazione.
6.3 Il Referente privacy stabilità se c'è qualcosa che può essere fatto per recuperare eventuali perdite e limitare il danno che la violazione potrebbe causare.
6.4 Il Referente privacy informerà la Direzione generale, il C.d.A. ed il Responsabile per la protezione dei dati (D.P.O.) ed unitamente a questi stabilirà chi potrebbe dover essere informato (O.d.V., Garante per la protezione dei dati personali, interessati al trattamento) e informerà, se del caso, la polizia.

**7 Valutazione del rischio**

7.1 Il Referente privacy, entro 24 ore dal rapporto -di concerto con il D.P.O. e se del caso con il supporto del Referente IT e dell'Amministratore di Sistema- esaminerà la violazione e valuterà i rischi ad essa associati, ad esempio le potenziali conseguenze negative per gli individui, quanto gravi o sostanziali siano e quanto probabilmente si verificheranno.

7.3 L'esame dovrà tenere conto di quanto segue:

- il tipo di dati coinvolti;
- la loro sensibilità;
- le protezioni adottate (ad es. crittografia);
- cosa è successo ai dati, sono stati persi o rubati;
- se i dati potrebbero essere utilizzati in modo illegale o inappropriato;
- chi sono gli individui, numero di persone coinvolte e potenziali effetti su tali soggetti interessati;
- se ci sono conseguenze più ampie sulla violazione.

**8 Notifica e comunicazione**

8.1 La Direzione generale, sentiti il Referente privacy, se del caso il responsabile del settore IT e l'Amministratore di Sistema, ed il D.P.O., determinerà chi deve essere informato della violazione.

8.2 Ogni incidente sarà valutato caso per caso; tuttavia, sarà necessario considerare quanto segue:

- se ci sono prescrizioni legali/contrattuali che impongano una notifica;
- se l'eventuale comunicazione potrebbe aiutare la persona interessata al fine di mitigare i rischi;
- se l'eventuale comunicazione potrebbe essere di aiuto al fine di aiutare a prevenire l'uso non autorizzato dei dati personali?
- se la comunicazione è prescritta dal GDPR.

8.3 L'eventuale comunicazione alle persone i cui dati personali sono stati interessati dall'incidente avverrà, ove necessario, senza giustificato ritardo e includerà una descrizione di come e quando si è verificata la violazione e i dati coinvolti. Verranno forniti consigli specifici e chiari su ciò che possono fare per proteggersi e includere le azioni già intraprese per mitigare i rischi. Alle persone interessate saranno inoltre forniti dei recapiti con cui sarà possibile contattare il Titolare per ulteriori chiarimenti circa l'accaduto.

8.4 La comunicazione alle persone i cui dati personali sono stati interessati dall'incidente non è richiesta se è soddisfatta una delle seguenti condizioni:

a) il data breach non è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche coinvolte;
b) sono state adottate adeguate misure di protezione e tali misure tecniche e organizzative sono applicate ai dati personali oggetto della violazione, rendendo i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
c) sono state successivamente adottate misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
d) 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.

8.5 La notifica al Garante privacy è prescritta salvo sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Effettuata questa valutazione il Referente privacy curerà (sentito ove opportuno il responsabile del settore IT) entro 72 ore dal data breach, la sua notifica al Garante, secondo le modalità di cui all'art. 33 GDPR e utilizzando l'apposita procedura disponibile sul sito web dell'Autorità.
8.6 La Direzione generale, sentiti il Referente privacy, se del caso il responsabile del settore IT e l'Amministratore di Sistema, ed il D.P.O., deve prendere in considerazione l'eventuale comunicazione a terzi come la polizia, gli assicuratori, le società bancarie o delle carte di credito e i sindacati. Ciò sarebbe appropriato laddove l'attività illecita è nota o si ritiene che si sia verificata, o laddove sussista il rischio che in futuro possano verificarsi attività illegali.
8.7 La Direzione generale, sentito il Referente privacy, valuterà se debba essere rilasciato un comunicato stampa e sarà pronto a gestire qualsiasi richiesta di stampa in arrivo.

**9 Valutazione e risposta**

9.1 Una volta che il sinistro è stato contenuto, il Referente privacy, se del caso con il supporto del responsabile del settore IT e dell'Amministratore di Sistema, effettueranno una relazione completa delle cause della violazione e valuterà l'efficacia della risposta e le eventuali modifiche ai sistemi, politiche e procedure che dovrebbero essere intraprese.
9.2 La relazione dovrà essere presentata al D.P.O. per osservazioni.
9.3 I controlli esistenti saranno rivisti per determinare la loro adeguatezza e se debbano essere intraprese azioni correttive per minimizzare il rischio che si verifichino incidenti simili.
9.4 La relazione prenderà in considerazione:

- dove e come vengono conservati i dati personali, dove e come sono archiviati;
- dove risiedono i maggiori rischi e individuerà eventuali ulteriori punti deboli all'interno delle misure esistenti;
- se i metodi di trasmissione sono sicuri; condivisione della quantità minima di dati necessari;
- l'identificazione dei punti deboli all'interno delle misure di sicurezza esistenti;
- la consapevolezza del personale e dei collaboratori;
- l'implementazione di un piano di violazione dei dati e identificazione di un gruppo di individui responsabili di reagire alle segnalazioni di violazioni della sicurezza.

9.5 La relativa relazione dovrà essere inviata alla Direzione generale, che valuterà quali modifiche si rendano opportune.

**ALLEGATO 1**

| **COMUNICAZIONE DI UNA VIOLAZIONE** | **DA COMPILARE A CURA DEL SEGNALANTE** |
|---|---|
| Data in cui è stato scoperto la violazione: | |
| Prevedibile data in cui è avvenuta una violazione: | |

| | |
|---|---|
| Luogo della violazione: | |
| Nome della persona che segnala una violazione: | |
| Dati di contatto della persona che segnala l'incidente: | |
| Breve descrizione della violazione o dettagli delle informazioni perse e/o del danno occorso: | |
| Numero di soggetti interessati, se noti: | |
| Alcuni dati personali sono stati messi a rischio? In caso di risposta affermativa, si prega di fornire dettagli: | |
| Breve descrizione di ogni azione intrapresa al momento della scoperta:<br><br>Notifica [ ]<br><br>Comunicazione [ ] | |

## D - Strumenti informatici

**1 Introduzione**

1.1 La presente policy regola l'utilizzo degli strumenti informatici (quali PC, laptop, tablet, smartphone, email, gestionali, etc.) messi a disposizione dal Titolare a dipendenti e collaboratori e va sottoposta agli stessi all'atto della consegna dello strumento informatico.

1.2 Va innanzitutto premesso che tutti gli strumenti messi a disposizione dal Titolare, salvo non sia espressamente indicato un diverso fine, devono intendersi messi a disposizione dei lavoratori unicamente per svolgere la propria attività lavorativa e dei collaboratori unicamente per svolgere la propria attività di collaborazione.

**2 Scopo**

2.1 Il Titolare è obbligato, ai sensi del Reg. UE n. 2016/679 (GDPR) a garantire la sicurezza di tutti i dati personali durante il loro trattamento.

2.2 La presente policy definisce la procedura da seguire per garantire la sicurezza degli strumenti informatici del Titolare, che contengono o possono contenere dati personali trattati dallo stesso.

2.3 La presente policy deve considerarsi integrativa delle nomine o incarichi/autorizzazioni sottoposte al dipendente/collaboratore. In caso di difformità fra la presente policy e le istruzioni ricevute dal singolo dipendente/collaboratore, queste ultime devono prevalere.

**3 Obiettivo**

3.1 La presente policy si riferisce a tutti i dati personali, particolari e giudiziari detenuti dal Titolare in formato informatico. Per "**dato personale**" si considera 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 (art. 4 Reg. UE 2016/679).

3.2 L'obiettivo di questa policy è garantire la sicurezza del trattamento dei dati sugli strumenti informatici del Titolare, ai sensi dell'art. 32 del GDPR, il quale prescrive che: "Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio".

**4.0 Gestione dei PC/Laptop**

4.1 Nel caso in cui al dipendente/collaboratore sia assegnato o affidato in uso (anche temporaneo) un PC/Laptop, lo stesso è tenuto ad utilizzarlo unicamente per ragioni lavorative/connesse all'incarico/connesse al rapporto di collaborazione.

4.2 I PC/Laptop in uso sono sottoposti ad autenticazione personale dell'utente, con password composte di almeno otto caratteri alfanumerici. L'utente dovrà provvedere a modificare la password almeno ogni sei mesi.

4.3 La password deve essere mantenuta segreta dall'utente, adottando gli opportuni accorgimenti per la sua custodia, fatta unicamente eccezione per concedere l'accesso al PC/Laptop ogniqualvolta ciò sia necessario per aggiornamenti, verifiche o ispezioni.

4.4 Nel caso di attivazione di sistemi di autenticazione multifattore le disposizioni di cui al punto 4.3 si applicano, in quanto compatibili, allo strumento dedicato all'autenticazione multifattore.

4.5 Non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione esplicita da parte del Titolare o da suo delegato espressamente individuato, in quanto sussiste il grave pericolo di installare strumenti che mettono a rischio la sicurezza della struttura informatica del Titolare (specie con riguardo ai PC/Laptop connessi in rete con il server).

4.6 Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal Titolare. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'azienda a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software.
4.7 Non è consentito all'utente modificare le impostazioni del PC/Laptop assegnato in uso, fatto salvo per modifiche relative alle preferenze in tema di aspetto/periferiche di input (mouse/tastiera) utilizzando comunque solo risorse disponibili sullo strumento, senza download di risorse o programmi o loro importazione dall'esterno.
4.8 Il PC/Laptop deve essere spento prima di lasciare gli uffici o in caso di assenze prolungate e deve essere dotato di blocco automatico dell'accesso entro un tempo massimo di 10 minuti di inattività.
4.9 Non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, unità di memoria rimovibile USB, ecc…), se non con l'autorizzazione espressa del Titolare o di un suo delegato espressamente individuato.
4.10 Si sottolinea comunque l'importanza di controllare metodicamente tutti i file provenienti dall'esterno e di adottare diligentemente le opportune cautele, al momento della eventuale trasmissione all'esterno di nostri file.

**5 Software di protezione**

5.1 L'utente è tenuto a verificare che sui PC/Laptop che gli vengono assegnati in uso siano abilitati ed aggiornati i software di protezione di cui dispone il Titolare. le cui specifiche tecniche sono disponibili aprendo i relativi programmi sul PC.
5.2 Con particolare riferimento ai dispositivi Laptop e/o ad altri dispositivi facilmente asportabili, sugli stessi va verificata l'attivazione dei sistemi di crittografia predisposti dal titolare.
5.3 Si segnala che, una volta attivato il sistema di crittografia predisposto dal titolare, lo smarrimento della password di accesso al dispositivo comporta la perdita dei dati e che, pertanto, la stessa andrà conservata con cura in luogo protetto e comunque **non** vicino e/o sul dispositivo, venendo meno in tal modo l'obiettivo di sicurezza che ci si prefigge di raggiungere con la crittografia del sistema.
5.3 Eventuali periferiche di archiviazione rimuovibili dovranno essere sottoposte a identico procedimento di crittografia, salvo dovessero essere autorizzati ulteriori software con identico livello di sicurezza.

**6 Gestione Smartphone/Tablet**

6.1 Nel caso in cui al dipendente/collaboratore sia assegnato o affidato in uso (anche temporaneo) un dispositivo Smartphone/Tablet, lo stesso è tenuto ad utilizzarlo unicamente per ragioni lavorative/connesse all'incarico/connesse al rapporto di collaborazione.
6.2 I dispositivi Smartphone/Tablet in uso sono sottoposti ad autenticazione personale dell'utente, con password composte di almeno otto caratteri alfanumerici. L'utente dovrà provvedere a modificare la password almeno ogni sei mesi.
6.3 La password deve essere mantenuta segreta dall'utente, adottando gli opportuni accorgimenti per la sua custodia, fatta unicamente eccezione per concedere l'accesso al dispositivo ogniqualvolta ciò sia necessario per aggiornamenti, verifiche o ispezioni.
6.4 Nel caso di attivazione di sistemi di autenticazione multifattore le disposizioni di cui al punto 6.3 si applicano, in quanto compatibili, allo strumento dedicato all'autenticazione multifattore.
6.5 Non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione esplicita da parte del Titolare o da suo delegato espressamente individuato.

6.6 Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal Titolare. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'azienda a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software.
6.7 Non è consentito all'utente modificare le impostazioni del dispositivo assegnato in uso, fatto salvo per modifiche relative alle preferenze in tema di aspetto, utilizzando comunque solo risorse disponibili sullo strumento, senza download di risorse o programmi o loro importazione dall'esterno.
6.8 Il dispositivo deve essere configurato in modo che le notifiche non risultino visibili prima dello sblocco del dispositivo.
6.9 Si sottolinea comunque l'importanza di controllare metodicamente tutti i file provenienti dall'esterno e di adottare diligentemente le opportune cautele, al momento della eventuale trasmissione all'esterno di nostri file.
6.10 L'utente è tenuto a verificare che sui dispositivi che gli vengono assegnati in uso siano abilitati ed aggiornati i software di protezione di cui dispone il Titolare. le cui specifiche tecniche sono disponibili aprendo i relativi programmi sul dispositivo.
6.11 L'utente è tenuto a verificare che sul dispositivo sia attivata la crittografia dei dati (dal menù "Impostazioni") e ad attivarla nel caso in cui non lo fosse. Ove siano presenti unità esterne (SD) sul dispositivo (il cui utilizzo è comunque subordinato alla previa autorizzazione da parte del titolare), anche queste andranno crittografate.

**7 Uso di dispositivi propri**

7.1 Qualora il dipendente/collaboratore venga autorizzato (procedura di cui deve risultare previa evidenza scritta) ad utilizzare dispositivi propri per trattare i dati personali di competenza del Titolare, lo stesso è tenuto a rispettare i contenuti della presente policy, in quanto compatibili (in particolare si segnala la necessità di crittografare tutti i dispositivi mobili/laptop). Non è in ogni caso ammesso l'utilizzo di dispositivi "condivisi" fra più soggetti.
7.2 I dati personali andranno cancellati dal dispositivo una volta trasferiti su dispositivi/server del Titolare e comunque non appena gli stessi non saranno più necessari per l'espletamento dell'attività assegnata al dipendente/collaboratore.
7.3 L'utilizzo del dispositivo per le finalità rappresentate nella presente policy impone comunque al dipendente/collaboratore di osservare, nel momento della dismissione del dispositivo utilizzato, le procedure prescritte dal Garante Privacy nel provvedimento del 13 ottobre 2008 in materia di dismissione di pc e dispositivi elettronici [1571514], nonché di collaborare con il Titolare nel caso in cui sia necessario evadere richieste degli interessati (es. accessi, rettifiche o cancellazioni di dati).
7.4 Viene in particolare richiesto al dipendente/collaboratore di effettuare una procedura di eliminazione dei dati attraverso software appositi, attivando gli opportuni accorgimenti tecnici idonei a cancellare in maniera definitiva i dati personali memorizzati così da garantire la loro non intelligibilità.

**8 Software gestionali**

8.1 Nel caso in cui al dipendente/collaboratore sia consentito accesso (anche temporaneo) ad un software gestionale in uso al Titolare, lo stesso è tenuto ad utilizzarlo unicamente per ragioni lavorative/connesse all'incarico/connesse al rapporto di collaborazione.
8.2 I software gestionali in uso al Titolare sono sottoposti ad autenticazione personale ed individuale dell'utente, con password composte di almeno otto caratteri alfanumerici. L'utente dovrà provvedere a modificare la password almeno ogni sei mesi.

8.3 La password deve essere mantenuta segreta dall'utente, adottando gli opportuni accorgimenti per la sua custodia, fatta unicamente eccezione per concedere l'accesso al software gestionale ogniqualvolta ciò sia necessario per aggiornamenti, verifiche o ispezioni.
8.4 Nel caso in cui, per le caratteristiche del software gestionale, non sia possibile un'autenticazione personale dell'utente, la password verrà fornita dal Titolare o da suo delegato espressamente individuato e verrà da questi variata ogni sei mesi, salvo espressa deroga (di cui deve risultare previa evidenza scritta).

**9 Email**

9.1 Nel caso in cui al dipendente / collaboratore sia fornita una **casella di posta elettronica individualizzata** (es. nome.cognome@funiviedelbaldo.it), lo stesso è tenuto ad utilizzarlo unicamente per ragioni lavorative/connesse all'incarico/connesse al rapporto di collaborazione.
9.2 L'utente è informato che sia i messaggi ricevuti, che quelli spediti, saranno leggibili anche da altri soggetti appartenenti al Titolare o suoi dipendenti: ciò è necessario per garantire un regolare funzionamento dell'attività aziendale, soprattutto nei giorni di assenza dell'utente.
9.3 L'utente dovrà reimpostare la password della casella una volta che la stessa gli verrà concessa in uso, dandone avviso al Titolare o a suo delegato espressamente individuato. Successivamente l'utente dovrà provvedere a modificare la password almeno ogni sei mesi dandone avviso al Titolare o a suo delegato espressamente individuato.
9.4 La password deve essere mantenuta segreta dall'utente, adottando gli opportuni accorgimenti per la sua custodia, fatta unicamente eccezione per concedere l'accesso alla casella email ogniqualvolta ciò sia necessario per verifiche o ispezioni.
9.5 Nel caso in cui, all'utente venga assegnata in uso una casella email che, per le sue caratteristiche, deve rimanere condivisa fra più soggetti (es. la casella info@funiviedelbaldo.it o la casella PEC del Titolare), la password verrà fornita dal Titolare o da un suo delegato espressamente individuato e verrà da questi variata ogni sei mesi (nel caso il delegato dovrà comunque informare gli ulteriori autorizzati all'accesso del cambio password e delle credenziali adottate).
9.6 Anche in questo caso, ed a maggior ragione, l'utente è informato che sia i messaggi ricevuti, che quelli spediti, saranno leggibili anche da altri soggetti appartenenti al Titolare o suoi dipendenti.
9.7 Nell'utilizzo delle caselle email o PEC si raccomanda la massima attenzione nell'apertura della corrispondenza, in particolare quando la stessa contiene link e/o file allegati. Prima di procedere all'apertura di file o link "sospetti"[1], si raccomanda di dare avviso della circostanza al Referente privacy (raggiungibile all'email privacy@funiviedelbaldo.it).
9.8 Il cestino deve essere periodicamente cancellato e non può in ogni caso mantenere posta per oltre 30 giorni. Si comunica che le mail più vecchie di 10 anni dovranno essere cancellate salvo sussistano specifiche esigenze che ne giustificano la conservazione (da effettuare anche su server estraendo il file .eml), le mail più vecchie di 10 anni potranno in ogni caso essere automaticamente cancellate senza preavviso.
9.9 In caso di assenza improvvisa o prolungata, ove per improrogabili necessità legate all'attività lavorativa si debba conoscere il contenuto dei messaggi di posta elettronica in relazione ad una casella email relativa ad un soggetto identificato (caselle email individualizzate) o identificabile (caselle email assegnate ad un solo individuo), il dipendente / collaboratore

[1] Quanto ai file allegati, va prestata attenzione in particolare ai file con estensioni .exe, .com, .vbs, .htm, .scr, .bat, .js, .pif, ma non va dimenticato che anche estensioni all'apparenza innocue possono nascondere contenuti malevoli.
Quanto ai link è importante verificare la corrispondenza fra il testo del link e l'indirizzo a cui rimanda (passando con il mouse sopra il link), attenzione in particolare ad individuare il dominio reale cui rimanda il link: "google.com/xyz/…" è una pagina su dominio google.com, mentre "google.com.xyz.xy/…" è una pagina su dominio xyz.xy, quindi non affidabile.

potrà delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività verrà redatto apposito verbale e verrà informato il lavoratore interessato alla prima occasione utile. Ove il lavoratore non abbia provveduto ad individuare per iscritto un fiduciario, all'accesso sarà competente il Referente privacy aziendale, che stenderà apposito verbale ed informerà il lavoratore interessato alla prima occasione utile.

9.10 In caso di cessazione del rapporto lavorativo e /o di collaborazione, l'azienda darà corso entro sei mesi alla cancellazione dei dati contenuti nella casella email (salvo circostanze eccezionali giustifichino il prolungamento della conservazione). Ove per improrogabili necessità legate all'attività lavorativa si debba conoscere il contenuto dei messaggi di posta elettronica in relazione ad una casella email relativa ad un soggetto identificato (caselle email individualizzate) o identificabile (caselle email assegnate ad un solo individuo), il dipendente / collaboratore potrà effettuare direttamente l'inoltro della corrispondenza inevasa ovvero delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale ultima attività verrà redatto apposito verbale e verrà informato il lavoratore interessato alla prima occasione utile. Ove il lavoratore non abbia provveduto ad individuare per iscritto un fiduciario, e/o comunque l'azienda abbia documentate ragioni per non ritenere completo l'inoltro effettuato, all'accesso sarà competente il Referente privacy aziendale, che stenderà apposito verbale ed informerà il lavoratore interessato alla prima occasione utile.

**10 Connessione da esterno**

10.1 Ai fini della presente policy, le connessioni da esterno comprendono tutte le connessioni non direttamente effettuate alla rete aziendale e che accedono a dispositivi inclusi nel perimetro aziendale.

10.2. In caso di connessione da esterno è obbligatorio accedere alla rete sempre tramite connessioni VPN (messe a disposizione dal Titolare) e l'utente ha la responsabilità di garantire, alla connessione via VPN, la stessa attenzione e diligenza applicata ad una connessione diretta.

10.3 Non è ammessa la connessione alla rete aziendale di dispositivi di terze parti. Qualora in casi eccezionali e comunque previa espressa autorizzazione del responsabile del settore IT e dal Referente privacy (che documenti i motivi dell'eccezione), i dispositivi, in tale fase, rappresenteranno una estensione della rete aziendale e come tali andranno soggetti alle norme e procedure previste nella presente policy.

10.4 In particolare l'utilizzo del dispositivo e degli accessi è consentito nei limiti degli incarichi assegnati, il PC deve essere dotato di password di almeno otto caratteri variata a cadenza semestrale e mantenuta segreta, deve essere dotato di blocco automatico dell'accesso entro un tempo massimo di 10 minuti di inattività, deve essere aggiornato e dotato di software di protezione anch'essi aggiornati e deve essere crittografato (se laptop).

**11 Controllo a distanza**

11.1 Si precisa che non sono installati o configurati sui sistemi informatici in uso agli utenti apparati hardware o strumenti software aventi come scopo il controllo a distanza dell'attività dei lavoratori.

11.2 Va comunque precisato che i log relativi all'utilizzo degli strumenti informatici, reperibili nella memoria degli stessi ovvero sui server o sui router dell'Ente, nonché i file con essi trattati, sono registrati e possono essere oggetto di controllo da parte dell'Ente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'organizzazione.

11.3 In caso di anomalie, il Titolare, per quanto possibile, privilegerà preliminari controlli anonimi e quindi riferiti a dati aggregati nell'ambito di intere strutture lavorative o di sue aree nelle quali si è verificata l'anomalia.
11.4 In tali casi, il controllo si concluderà con un avviso all'ufficio interessato in cui è stato rilevato l'utilizzo anomalo degli strumenti affinché lo stesso inviti le strutture da lui dipendenti ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.
11.5 In caso di circostanze eccezionali, ovvero in caso di successive, perduranti anomalie, il Titolare si riserva di effettuare verifiche anche su base individuale, comunque finalizzate esclusivamente alla individuazione di eventuali condotte illecite.
11.6 Dette verifiche verranno comunque effettuate nel rispetto dei principi in tema di trattamento dati, e comunque minimizzando il trattamento effettuato, sia nell'estensione che nella durata. Ove possibile e compatibile con le esigenze di verifica, l'utente soggetto alla stessa verrà preavvertito dell'attività. o se questi controlli vengono effettuati indicare le modalità con cui verranno svolti in modo che i dipendenti siano sempre informati.

**12 Cessazione del rapporto di lavoro/ collaborazione**
12.1 Si precisa in caso di cessazione del rapporto lavorativo, ovvero al termine del rapporto di collaborazione, le credenziali per l'accesso agli strumenti, ai gestionali ed alle email del Titolare dovranno essere cambiate.
13.2 La casella email individualizzata (es. nome.cognome@funiviedelbaldo.it) dovrà invece essere disattivata curando che il sistema generi una risposta automatica al mittente, informando che la casella di posta elettronica è stata disattivata.

**13 Rinvii**
13.1 Per quanto non disciplinato nella presente policy si rinvia alle ulteriori policy adottate dal Titolare nonché agli incarichi / nomine ricevute.
13.2 In caso di ulteriori dubbi o incertezze operative è possibile rivolgersi al Referente privacy (raggiungibile all'email privacy@funiviedelbaldo.it) ovvero, in caso di residui dubbi, al D.P.O.

## E – Gestione sito e profili social media

**1 Introduzione**
La presente policy regola l'inserimento e diffusione di contenuti sul sito web istituzionale dell'azienda (https:// www.funiviedelbaldo.it) nonché sulle piattaforme social gestite dalla stessa o dalle sue articolazioni.
**2 Scopo**
2.1 L'azienda è obbligata, ai sensi del Reg. UE n. 2016/679 (GDPR) a garantire la minimizzazione del trattamento dei dati personali, evitando, specie nella diffusione dei dati sulla rete internet, di condividere più dati di quanto non sia necessario.
2.2 Al contempo l'azienda è tenuta a diffondere i dati personali in maniera lecita, ottenendo il consenso degli interessati salvo la normativa consenta il trattamento anche in difetto di consenso.
2.3 La presente policy definisce la procedura da seguire per garantire la liceità del trattamento e la minimizzazione dei dati nell'utilizzo di strumenti o piattaforme web.

La presente policy deve considerarsi integrativa delle nomine o incarichi/autorizzazioni sottoposte al dipendente / consulente. In caso di difformità fra la presente policy e le istruzioni ricevute dal singolo dipendente / consulente, queste ultime devono prevalere.

**3. Obiettivo**

La presente policy si riferisce a tutti i dati personali, particolari e giudiziari che l'azienda dovesse condividere online attraverso i propri canali istituzionali. Per "**dato personale**" si considera 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 (art. 4 Reg. UE n. 2016/679).

**4. Pubblicazioni sul sito web**

4.1 Nel caso in cui al dipendente/consulente sia assegnato o affidato il compito di inserimento dati/contenuti sul sito web del titolare, lo stesso è tenuto a verificare la legittimità dell'inserimento dei contenuti in relazione alla normativa in tema di dati personali.

4.2 In generale, ove l'obiettivo della pubblicazione possa essere raggiunto anche condividendo meno dati rispetto a quelli proposti in diffusione, l'incaricato è tenuto a segnalarlo all'azienda, suggerendo una pubblicazione meno invasiva.

4.3 La diffusione del dato è ammessa solo nella misura in cui sia necessaria per l'adempimento di un contratto o di un obbligo di legge, ovvero è subordinata al legittimo interesse del titolare (es. nella documentazione di un evento pubblico in cui siano ritratti personaggi noti o nel caso di fotografie di contesto che includano soggetti partecipanti all'evento pubblico) ovvero infine, nel caso in cui il legittimo interesse dell'azienda non prevalga rispetto alla riservatezza dell'individuo rappresentato, al **consenso, documentato, da parte dell'interessato** alla diffusione dei propri dati personali.

4.4 In particolare, la diffusione di **video o immagini** che ritraggono persone individuabili sul sito web dell'azienda deve passare per l'accertamento della sussistenza del legittimo interesse (immagini di contesto e di eventi pubblici, e comunque tenendo conto, anche in tale caso, della necessità di preservare la dignità ed il decoro dei soggetti ritratti) e, in caso lo stesso non sussista, per l'accertamento dell'acquisizione del consenso alla pubblicazione da parte di tutti i soggetti individuabili ritratti.

4.5 La diffusione di **video o immagini** che ritraggono **persone minori** sul sito web dell'azienda deve passare per l'accertamento dell'acquisizione del consenso alla pubblicazione da parte degli esercenti la potestà genitoriale di tutti i soggetti individuabili ritratti.

4.6 Per la pubblicazione di **video o immagini** che ritraggono persone individuabili va tenuto conto anche della disciplina in tema di diritto d'autore che, all'art. 97, prevede la necessità del consenso della persona ritratta salvo la riproduzione dell'immagine sia giustificata dalla notorietà o dall'ufficio pubblico coperto, da necessità di giustizia o di polizia, da scopi scientifici, didattici o culturali, ovvero quando la riproduzione è collegata a fatti, avvenimenti, cerimonie di interesse pubblico o svoltisi in pubblico.

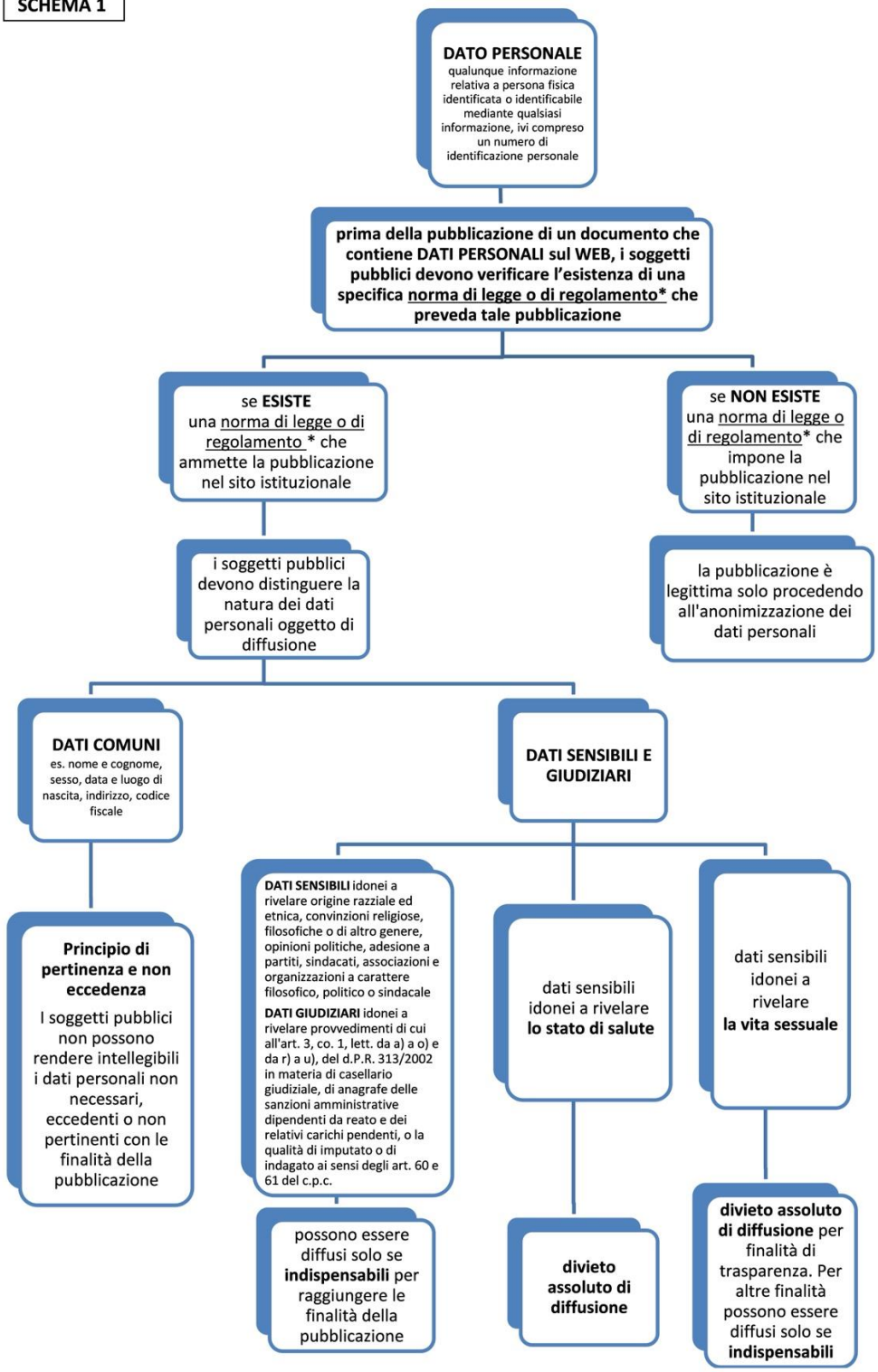
4.7 Va in ogni caso evitata la diffusione di **dati appartenenti a categorie particolari** (dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona) **ovvero relativi a condanne penali o reati**.

**5 Sezione amministrazione trasparente**

5.1 Quanto alle prescrizioni circa la pubblicazione di contenuti in questa sezione si rimanda alle Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati adottate dal Garante privacy e pubblicate sulla Gazzetta Ufficiale n. 134 del 12 giugno 2014).

5.2 Si riporta, in particolare, lo schema operativo declinato dal Garante in tale provvedimento:

**SCHEMA 1**




* N.B. Si precisa che la diffusione di dati comuni è ammessa solo se prevista da una norma di legge o di regolamento, mentre la diffusione di dati sensibili o giudiziari è ammessa se prevista espressamente solo da una norma di legge.

5.3 Va ricordato infine che la durata del periodo di pubblicazione è prevista per legge per un periodo di 5 anni, decorrenti dal 1° gennaio dell'anno successivo a quello da cui decorre l'obbligo di pubblicazione, ed è suscettibile di estensione unicamente nel caso in cui gli atti pubblicati producano, a tale data, i loro effetti.

**6 Pubblicazioni sui social**

6.1 Nel caso in cui al dipendente/consulente sia assegnato o affidato il compito di inserimento dati/contenuti sui social network gestiti dall'azienda o da sue articolazioni, lo stesso è tenuto a verificare la legittimità dell'inserimento dei contenuti in relazione alla normativa in tema di dati personali.

6.2 In generale, ove l'obiettivo della pubblicazione possa essere raggiunto anche condividendo meno dati rispetto a quelli proposti in diffusione, l'incaricato è tenuto a segnalarlo all'azienda, suggerendo una pubblicazione meno invasiva.

6.3 Va tenuto in considerazione che l'azienda non ha alcun obbligo di pubblicazione/condivisione di contenuti sui social network e che la diffusione di dati personali su tali piattaforme non può quindi generalmente trovare legittimazione nella normativa relativa ad obblighi contrattuali o legali.

6.4 La diffusione dei dati personali sui canali social dell'azienda è ammessa nei limiti di quanto disposto al punto 4 che precede, in quanto applicabile.

**7 Rinvii**

7.1 Per quanto non disciplinato nella presente policy si rinvia alle ulteriori policy adottate dall'azienda nonché agli incarichi / nomine a responsabile ricevute.

7.2 In caso di ulteriori dubbi o incertezze operative è possibile rivolgersi all'indirizzo e-mail privacy@funiviedelbaldo.it ovvero al D.P.O.