



Privacy Policy

Ultimo aggiornamento del 5 luglio 2019

Indice

1.	Premessa - Il Gruppo Ascopiave	3
2.	Introduzione.....	3
3.	Scopo del documento.....	4
4.	Principi Generali	5
5.	Definizioni.....	6
6.	Ruoli e Responsabilità.....	12
6.1	Titolare del trattamento.....	13
6.2	Soggetto Delegato (o Soggetto con funzioni di Titolare)	15
6.3	Responsabile della Protezione dei Dati (RPD) o Data Protection Officer (DPO).....	15
6.4	Referente Privacy.....	15
6.5	Persona autorizzata al trattamento dei dati personali (o “Autorizzato”, o “Incaricato”)	16
6.6	Focal Point	18
6.7	Funzione Privacy.....	19
6.8	Responsabili esterni del trattamento dei dati personali	19
6.9	Amministratore di Sistema.....	19
6.10	Amministratore dei sistemi di videosorveglianza.....	20
7.	Diritti dell’interessato	20
8.	Adempimenti generali per il trattamento dei dati personali	22
8.1	Informative	22
8.2	Base giuridica del trattamento	22
8.3	Finalità previste	22
8.4	Riservatezza del trattamento dei dati e loro classificazione	23
8.5	Categorie particolari di Dati personali.....	23
8.6	Registro dei trattamenti	24
8.7	Data Breach e flussi comunicativi all’Autorità	25
8.8	Data Protection Impact Assessment e misure di sicurezza.....	25
8.9	Formazione	26
8.10	Trasferimento di dati personali	26
8.11	Cooperazione con l’Autorità di controllo – Gestione delle istanze in materia di Privacy ...	26
8.12	Monitoraggio della conformità.....	27
9.	Attività peculiari - Marketing e Profilazione	27

1. Premessa - Il Gruppo Ascopiave

Ascopiave S.p.A., con sede legale in Pieve di Soligo (TV), via Verizzo 1030 (di seguito “**Ascopiave**”) è una società che opera nel settore energetico, con particolare riguardo alla distribuzione di gas naturale ed alla vendita di gas ed energia elettrica. La stessa è a capo dell’omonimo Gruppo societario.

Il Gruppo detiene concessioni e affidamenti diretti per la gestione dell’attività di distribuzione in 230 Comuni, fornendo il servizio ad un bacino di utenza multiregionale di circa 1,5 milioni di abitanti, attraverso una rete di distribuzione che si estende per più di 10.000 chilometri.

L’attività di vendita di gas naturale ed energia elettrica è svolta attraverso diverse società, alcune a controllo congiunto, con una capillare presenza di uffici commerciali.

Ascopiave S.p.A., in particolare, controlla 5 società di vendita e 4 società di distribuzione del gas metano, tutte sul territorio Italiano:

Società di Vendita:

- Ascotrade S.p.A.;
- Etra Energia S.R.L.;
- Blue Meta S.p.A.;
- Amgas Blu S.R.L.;
- Ascopiave Energie S.p.A.;

Società di Distribuzione:

- AP Reti Gas S.p.A.;
- AP Reti Gas Vicenza S.p.A.;
- AP Reti Gas Rovigo S.R.L.;
- Edigas Esercizio Distribuzione Gas S.p.A..

Altre Società (rilevanti ai fini del presente Manuale):

- Asco Energy S.p.A. (controllata da Ascopiave);
- Asco Holding S.p.A. (che controlla Ascopiave);
- BIM Piave Nuove Energie S.R.L.

2. Introduzione

In data 25 maggio 2016 è stato approvato il Regolamento Europeo 2016/679 (Regolamento generale sulla protezione dei dati, di seguito il “Regolamento” o il “GDPR”), direttamente applicabile in tutti gli stati rientranti nel perimetro Europeo dal 25 maggio 2018.

Il Regolamento, così come il D.Lgs. 196/2003, come modificato ed integrato dal D.Lgs. 101/2018, disciplina il trattamento dei dati che consentono di risalire, anche indirettamente, ad una persona

fisica. Pertanto, sono dati personali non solo i dati anagrafici di un soggetto, ma anche il codice cliente, il codice fiscale, l'indirizzo IP, la matricola dipendente, ecc.

La normativa sulla protezione dei dati personali, contenuta nel Regolamento, viene integrata dai provvedimenti del Garante Privacy (Autorità di Controllo sulla base del Regolamento) e dalle indicazioni interpretative fornite dal Gruppo dei Garanti Europei (Working Party Article 29).

Tutte le società e tutti coloro che svolgono un'attività che comporti delle relazioni con soggetti fisici dovranno attenersi a quanto previsto dalla normativa di cui sopra.

Pertanto, anche i dipendenti del Gruppo Ascopiave (di seguito, "Il Gruppo" o "Ascopiave") che trattino dati personali in ragione delle funzioni aziendali svolte sono tenuti a seguire la citata disciplina sulla protezione dei dati personali e ad attenersi, anzitutto, alla presente Privacy Policy (o "Manuale"), nonché, a seconda delle casistiche concrete, alle ulteriori specifiche Policy recanti la disciplina di dettaglio.

La normativa in materia di dati personali interessa anche l'utilizzo degli strumenti informatici forniti dalla società ai propri dipendenti (chiamate anche risorse informatiche aziendali), ormai sempre più necessarie per lo svolgimento dell'attività lavorativa. Infatti, nell'utilizzo di questi strumenti, si viene a contatto con informazioni riservate e personali.

A tal riguardo, nel corso del presente documento avranno particolare rilevanza anche le seguenti fonti normative:

- Provvedimento generale del Garante per la protezione dei dati personali del 5 marzo 2007, "Lavoro: linee guida del Garante per posta elettronica e internet";
- Documento del Gruppo di lavoro per la tutela dei dati ex art. 29 (Direttiva 96/45/EC) del 29 maggio 2002, riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro;
- L'art. 4 e 8 della Legge 300/1970 (c.d. Statuto Lavoratori).

L'obiettivo della presente Policy è quello di definire le regole e le linee guida per salvaguardare da usi impropri i "Dati Personali" (di seguito anche sinteticamente i "Dati") relativi alle persone fisiche, come definiti dal Regolamento, garantendo che il trattamento dei Dati si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'Interessato.

3. Scopo del documento

Scopo del documento è quello di riportare:

- le definizioni e i principi generali in materia di Privacy;
- i ruoli, le responsabilità e le nomine delle figure relative alla gestione delle tematiche "Privacy" nel contesto del Gruppo Ascopiave;
- i diritti riconosciuti agli interessati, di cui sono trattati i Dati, e le limitazioni al trasferimento dei medesimi;

- gli adempimenti generali per il trattamento dei Dati che la capo Gruppo ha stabilito per la sua organizzazione e per i soggetti presenti nel documento;
- le linee guida per il trattamento dei Dati e la gestione dei documenti.

In ottemperanza a quanto previsto dal GDPR, Ascopiave S.p.A. ha predisposto apposite Policy (da considerarsi parte integrante del presente Manuale), specificamente dedicate a:

- a. **Gestione delle richieste degli interessati riferite all'esercizio dei diritti previsti dal Regolamento UE 2016/679** (rif. art. 12 del Regolamento). Ogni Interessato ha diritto di accesso (art. 15), diritto di rettifica (art. 16), diritto all'oblio (art. 17), diritto di limitazione del trattamento (art. 18), diritto a vedersi notificare la rettifica, la cancellazione dei dati personali, o la limitazione del trattamento (art. 19), diritto alla portabilità dei dati (art. 20), diritto di opposizione al trattamento (art. 21), diritto a non essere sottoposto ad una decisione basata unicamente sul trattamento automatizzato (art. 22).
- b. **Privacy By Design** (art. 25). Il Titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate ad assicurare la protezione dei dati e la tutela dei diritti degli interessati, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso. Tali misure devono anche garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.
- c. **Data Breach** (violazione di dati personali – art. 33 e 34). Ogni evento dal quale deriva la perdita, la distruzione, la modifica, la divulgazione non autorizzata, o l'accesso abusivo a dati personali.
- d. **Data Protection Impact Assessment** (DPIA – art. 35). Conformemente al principio di Accountability e nei casi in cui il trattamento può presentare rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento è chiamato a valutare preventivamente le conseguenze che il trattamento dei dati potrebbe arrecare ai diritti e alle libertà dei soggetti cui i dati si riferiscono.
- e. **Data Retention**. Il Titolare del trattamento deve tenere conto di quanto prescritto dal GDPR in merito alle modalità e ai tempi di conservazione dei dati dei soggetti interessati.

Faranno altresì parte del presente Manuale anche le eventuali, ulteriori procedure operative, prassi, policy, ecc., pur successive all'emanazione di questo documento, che andranno a regolare nel dettaglio i processi inerenti alle tematiche privacy.

Il presente documento è adottato dal Titolare e diffuso all'interno dell'organizzazione.

4. Principi Generali

In attuazione dei principi dettati dalla Normativa anzidetta, ognuna delle società del Gruppo è tenuta ad assicurare la protezione dei Dati trattati nell'ambito della propria attività.

A tal fine Ascopiave adotta le misure tecniche e organizzative più adeguate a garantire l'effettivo rispetto delle garanzie e dei principi previsti in tema Privacy, nonché una appropriata copertura dei rischi di perdita dell'integrità, della riservatezza e della disponibilità delle informazioni personali di cui è in possesso.

Alla luce di quanto sopra, Ascopiave definisce i processi di trattamento dei Dati in modo che le operazioni materiali di trattamento degli stessi (raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, ecc.) avvengano nel rispetto dei principi generali in materia, i più rilevanti dei quali, sono qui di seguito sinteticamente descritti:

Principio di liceità, correttezza e trasparenza

I Dati devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.

Principio di limitazione della finalità

Devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità.

Principio di minimizzazione dei dati

I Dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

Principio di esattezza

I Dati devono essere esatti e, se necessario, aggiornati, devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.

Principio di limitazione della conservazione

I Dati vanno conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

Principio di integrità e riservatezza

I Dati vanno trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale.

5. Definizioni

Ai fini del presente Manuale e di tutte le policy e, in genere, i documenti connessi all'ambito "Privacy", trovano applicazione le seguenti definizioni. Per comodità di consultazione, le stesse sono esposte in ordine alfabetico.

Amministratore di Sistema	Persona fisica responsabile della gestione e manutenzione
----------------------------------	---

Gruppo Ascopiave – Privacy Policy

	di impianti di elaborazione con cui vengono effettuati trattamenti di Dati, compresi i sistemi di gestione delle basi di dati, i sistemi software, le reti locali e gli apparati di sicurezza informatica, nella misura in cui consentano di intervenire sui Dati.
Amministratore dei sistemi di videosorveglianza	Persona fisica responsabile della gestione degli impianti di videosorveglianza, nel rispetto dei principi applicabili al trattamento dei Dati personali di cui all'art. 5 del GDPR.
Archivio o Banca Dati	Qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico (art. 4, comma 1, n. 6 del Regolamento).
Autorità di controllo (o il "Garante")	E' il "Garante per la Protezione dei Dati Personali", organo collegiale, composto da quattro membri eletti dal Parlamento, i quali rimangono in carica per un mandato di sette anni non rinnovabile. Opera in piena autonomia e con indipendenza di giudizio e valutazione. Il Garante si occupa di tutti gli ambiti, pubblici e privati, nei quali occorre assicurare il corretto trattamento dei dati e il rispetto dei diritti delle persone connessi all'utilizzo delle informazioni personali.
Cancellazione o Distruzione di dati personali	Procedimento che porta alla definitiva e permanente cancellazione dei dati personali, rendendoli indisponibili per chiunque.
Categorie particolari di dati personali (o Dati particolari – ex dati sensibili)	Dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché [...] dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (art. 9, comma 1 del Regolamento).
Codice	Decreto Legislativo n. 196 del 30 giugno 2003, "Codice in materia di protezione dei dati personali" (aggiornato dal D.Lgs. 10 agosto 2018 n. 101) e s.m.i.
Data Breach	Ogni evento che comporta, accidentalmente o in modo

(o Violazione di dati personali)	illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata, o l'accesso abusivo ai dati personali trasmessi, conservati, o comunque trattati.
Data Protection Impact Assessment (DPIA)	Attività di valutazione delle conseguenze di un trattamento dei dati, che è obbligatoria, prima di procedere al trattamento, nel caso in cui ci sia rischio elevato per i diritti e le libertà delle persone fisiche (rif. art. 35 del Regolamento). In funzione dell'esito della valutazione vengono definite misure di sicurezza proporzionate al rischio del trattamento per mitigarlo in misura adeguata.
Dati "biometrici"	Dati personali ottenuti da un trattamento tecnico specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici (art. 4, comma 1, n. 14 del Regolamento).
Dati "genetici"	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 (art. 4, comma 1, n. 13 del Regolamento).
Dati comuni (o neutri)	Dati personali che non appartengono strettamente alla vita intima della persona, ma riguardano elementi quali le generalità, l'indirizzo, la residenza, il luogo di lavoro, ecc.
Dati giudiziari	Dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza (art. 10 del Regolamento). Rappresentano, nella sostanza, una peculiare categoria di Dati particolari.
Dati relativi alla salute	Dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute (art. 4, comma 1, n. 15 del Regolamento).
Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile ("Interessato") in base

Gruppo Ascopiave – Privacy Policy

	<p>all'elemento identificativo di cui si dispone, come il nome, il cognome, un numero o elemento di identificazione (numero telefonico, e-mail, indirizzo, ecc.), un dato di ubicazione (es. segnale da dispositivo gps), un identificativo online (es. account personale), o altri elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.</p>
Focal Point	<p>Soggetti designati (e nominati) da ogni Società del Gruppo, in ragione del loro ruolo strategico nell'ambito delle singole organizzazioni aziendali, con il compito di sovrintendere ai progetti ed alle attività societarie che abbiano e/o possano avere incidenza sul trattamento di Dati personali.</p> <p>I Focal Point provvedono, altresì, quale primo riporto, alle valutazioni ed alla costante informativa, nonché alla tempestiva allerta della Funzione Privacy, rispetto alle situazioni di maggior rilievo (tra cui, in particolare, i Data Breach).</p>
Funzione Privacy	<p>È un organismo designato da Ascopiave, che ha, quali componenti stabili, il Soggetto Delegato ed il DPO di Ascopiave ed il Referente Privacy. L'organismo è il riferimento principale di tutti i Soggetti Incaricati dei trattamenti, per ogni rilevante aspetto, non meramente operativo, riguardante la protezione dei dati personali.</p> <p>A seconda delle esigenze, la compagine può essere integrata da altre funzioni (es. DPO di altra Società, Direzioni Legal e ICT, Focal Point, ecc.).</p> <p>L'organismo ha altresì la responsabilità specifica di garantire la gestione delle segnalazioni di violazione di dati personali (Data Breach).</p>
GDPR (o Regolamento)	<p>General Data Protection Regulation, è il Regolamento UE 2016/679 sulla protezione dei dati personali, pubblicato il 4 maggio 2016 ed entrato in vigore il 25 maggio 2018.</p>
Misure di sicurezza	<p>L'insieme delle misure tecniche ed organizzative volte a garantire la protezione dei dati personali, in modo da consentire il mantenimento (o l'implementazione) di un livello di sicurezza adatto al rischio proprio dei singoli</p>

Gruppo Ascopiave – Privacy Policy

	trattamenti.
Normativa	Si intende il Regolamento UE 2016/679, nonché ogni legge, o provvedimento avente efficacia di legge, o regolamento che disciplini la materia del trattamento dei dati personali ed ogni altro Provvedimento emesso dal Garante per la Protezione dei Dati Personali e/o dal WP 29 e/o dal Comitato Europeo.
Persona autorizzata al trattamento dei dati personali (anche “Autorizzato” o “Incaricato”)	Qualsiasi persona autorizzata a trattare Dati personali dal Titolare del trattamento, sotto la diretta autorità di quest’ultimo, attenendosi alle istruzioni da questi impartite (come previsto agli articoli 4, numero 10 e 29 del GDPR). La designazione è effettuata per iscritto e individua l’ambito del trattamento consentito.
Privacy	Ai fini del presente documento, nonché di ogni altra policy e/o regola di condotta connessa, è un’espressione generale ed omnicomprensiva rispetto alla tematica della tutela dei Dati personali, ai sensi della Normativa.
Profilazione	Qualsiasi forma di trattamento automatizzato di Dati personali consistente nell'utilizzo di tali Dati per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione, o gli spostamenti di detta persona (art. 4, comma 1, n. 4 del Regolamento).
Referente Privacy	È un soggetto, designato da Ascopiave con riferimento all’intero Gruppo, con adeguata conoscenza della Normativa e delle prassi in materia di protezione dei Dati. Il compito principale è di sovrintendere ai processi ed agli adempimenti in materia di Privacy, in collaborazione con il DPO, il Soggetto Delegato ed ogni altra funzione cui siano attribuite, in via continuativa o transitoria, mansioni e/o obbligazioni relative (o connesse) alla regolazione Privacy.
Registro dei trattamenti	E’ il Registro tenuto obbligatoriamente, in forma scritta, da ciascuna Società, ai sensi dell’art. 30 del Regolamento. La tenuta dei registri è di norma rimessa al Referente Privacy.

Gruppo Ascopiave – Privacy Policy

	Lo stesso provvede altresì all'aggiornamento e/o all'implementazione sulla base delle indicazioni in tal senso dei Focal Point.
Responsabile del trattamento (ex Responsabile esterno)	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, previo atto di nomina che definisce finalità, modalità, mezzi, ecc., tratta dati personali per conto del Titolare del trattamento (o dei Contitolari).
Responsabile della protezione dei dati (o Data Protection Officer - DPO)	È una figura introdotta dall'art. 37 del Regolamento (UE) 2016/679. Si tratta di un soggetto designato dal Titolare (o dal Responsabile) del trattamento per assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del Regolamento medesimo. Coopera con l'Autorità di controllo (il suo nominativo va comunicato al Garante) e costituisce il punto di contatto, anche rispetto agli Interessati, per le questioni connesse al trattamento dei Dati personali (artt. 38 e 39 del Regolamento).
Soggetto Delegato (o "Soggetto con funzioni di Titolare")	Soggetto individuato nell'ambito del management delle Società del Gruppo, designato dal Titolare, con apposito atto di nomina, al quale sono assegnate deleghe decisionali / rappresentative del Titolare medesimo in ambito Privacy.
Soggetto Interessato (o Interessato)	La persona fisica cui si riferiscono i dati personali. I Dati propri delle persone giuridiche (società, enti, ecc.) non sono soggetti al GDPR (e quindi alla Normativa privacy).
Titolare o Contitolare	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di Dati personali. Si ha "Contitolarità" quando la determinazione delle finalità e dei mezzi del trattamento sono determinati da due o più soggetti, in forza di uno specifico accordo in tal senso. In presenza di un rapporto di Contitolarità, gli obblighi normalmente in capo al Titolare si intendono riferiti a tutti i Contitolari (che, in merito, assumono responsabilità solidale).

	Del pari gli Interessati possono esercitare i loro diritti nei riguardi dell'uno o dell'altro Contitolare. Nel caso, ogni riferimento al Titolare è da ritenersi proprio anche del Contitolare.
Trattamento	Ai sensi dell'art. 4 del Regolamento è qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a Dati personali o insiemi di Dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento, 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.
Working Party Article 29 (o "WP 29")	Il gruppo di lavoro istituito ai sensi dell'art. 29 della Direttiva 95/46/EC.

6. Ruoli e Responsabilità

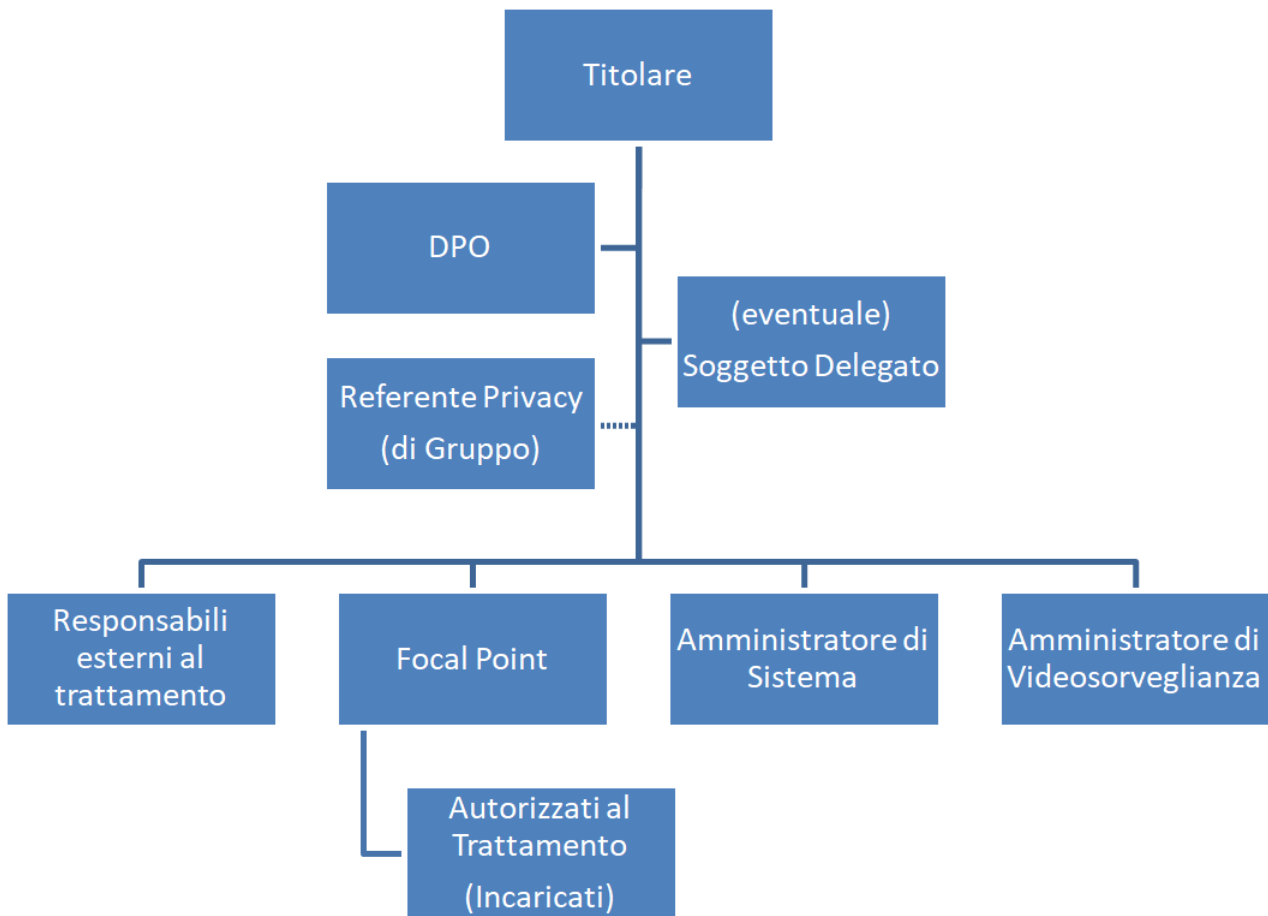
Al fine di presidiare il buon funzionamento del presente Manuale e di garantire gli adempimenti previsti dalla Normativa, Ascopiave, quale capo gruppo, ha individuato le seguenti figure (si rimanda alle definizioni di cui al paragrafo precedente):

- 1) Titolare del trattamento dei dati personali ("Titolare" o "Contitolare") [NB ogni società, relativamente ai trattamenti di propria competenza, assume la qualifica di Titolare];
- 2) Soggetto con funzioni di Titolare ("Soggetto Delegato");
- 3) Responsabile della Protezione dei Dati ("Data Protection Officer" o "DPO");
- 4) Referente Privacy;
- 5) Focal Point;
- 6) Autorizzato al trattamento dei Dati ("Incaricato");
- 7) Funzione Privacy;
- 8) Amministratore di sistema;
- 9) Amministratore dei sistemi di videosorveglianza;
- 10) Responsabile del trattamento dei dati personali ("Responsabile esterno").

Le figure di cui sopra, in funzione del proprio ruolo e delle proprie competenze, sono responsabili dell'applicazione dei contenuti del presente documento.

Nel seguente funzionigramma, si sintetizza lo schema adottato nel Gruppo per le finalità di

gestione degli aspetti privacy.



Il Referente Privacy, figura identificata dalla Capogruppo, cura la tenuta e l'aggiornamento (con verifica semestrale) dei funzionigramma di ogni Società (con specificazione dei Soggetti coinvolti). Nel proseguo, vengono descritte, per ogni ruolo, le principali responsabilità / pertinenze e le modalità di nomina.

6.1 Titolare del trattamento

Il Titolare è Ascopiave S.p.A. e/o le singole Società del Gruppo che operano in maniera autonoma e indipendente nel Trattamento dei Dati personali.

Nell'ambito dei rapporti infragruppo sono stati (o saranno) conclusi accordi di "Contitolarità", in forza dei quali, le funzioni di Titolare, relativamente ai dati personali trattati per la prestazione dei servizi infragruppo, sono svolte congiuntamente dalle Società del Gruppo.

Salva la designazione di un Soggetto Delegato, le attribuzioni del Titolare sono svolte dal legale rappresentante.

In generale, il Titolare (o Contitolare):

- definisce le finalità dei trattamenti dei Dati, nonché le tempistiche di conservazione degli stessi in relazione alle esigenze aziendali, conformemente a quanto prescritto dalla Normativa;

- assicura la formalizzazione e l'operatività del sistema di ruoli e responsabilità aziendali, coerentemente a quanto prescritto dalla Normativa, e ne garantisce la piena attuazione;
- sovrintende all'attuazione di specifici adempimenti previsti dalla Normativa, quali, in via esemplificativa, quelli attinenti a:
 - o informative, consensi e gestione dei riscontri all'Interessato;
 - o Registro dei Trattamenti;
 - o misure di sicurezza e gestione di eventuali Data Breach;
 - o Data Protection Impact Assessment (DPIA);
 - o formazione.

Più specificamente, il Titolare, per il tramite della propria organizzazione:

1. mette in atto misure tecniche e organizzative, sia in fase progettuale che all'atto del trattamento, adeguate ad assicurare (e a dimostrare) che il trattamento è effettuato conformemente a quanto prescritto dalla Normativa (es. nomina delle figure necessarie, attribuzione di vincoli e responsabilità, informative, procedure e istruzioni, misure di sicurezza, etc.), in modo tale che venga garantito un livello di sicurezza adeguato al rischio (ex art. 32 GDPR);
2. cura la verifica e l'aggiornamento delle misure tecniche e organizzative predette;
3. garantisce la liceità del trattamento e la tracciabilità del consenso al trattamento da parte degli Interessati;
4. assicura il riscontro alle richieste degli Interessati ex artt. 15-22 del GDPR;
5. fornisce agli Interessati le necessarie e opportune Informative in merito al trattamento (rif. artt. 13-14 del GDPR);
6. tiene ed aggiorna il Registro delle attività di trattamento ex art. 30 del GDPR;
7. provvede alle comunicazioni all'Autorità (ed eventualmente agli Interessati), ivi incluse quelle relative agli eventuali Data Breach ex art 33 del GDPR;
8. procede, quando necessario, alla valutazione d'impatto sulla protezione dei Dati (DPIA) e cura le eventuali comunicazioni, ex art 35-36 del GDPR;
9. richiede all'Autorità, curando i relativi iter procedurali, le autorizzazioni, i pareri e/o i nulla osta che abbiano a rendersi necessari per particolari Trattamenti;
10. inserisce nei contratti con soggetti terzi, specifiche clausole in materia di trattamento dei Dati, provvedendo altresì, ove necessario, alla designazione di Responsabili Esterni;
11. fornisce idonee istruzioni sul trattamento ai Responsabili Esterni designati;
12. designa il DPO ed assicura la pubblicazione dei dati di contatto, la relativa comunicazione all'Autorità ed il suo coinvolgimento nelle questioni riguardanti la Privacy.
13. predispone garanzie adeguate per il trasferimento dei Dati verso un paese terzo, o un'organizzazione internazionale.

6.2 Soggetto Delegato (o Soggetto con funzioni di Titolare)

Il Soggetto Delegato, ove nominato, esercita i poteri conferiti al Titolare in materia di trattamento dei Dati, nei limiti di quanto previsto dall'atto di nomina.

Il Soggetto Delegato di Ascopiave fa parte permanentemente della Funzione Privacy (al pari del DPO e del Referente Privacy).

6.3 Responsabile della Protezione dei Dati (RPD) o Data Protection Officer (DPO)

Il Data Protection Officer, con competenze in materia di misure di sicurezza ed adeguata conoscenza della Normativa, nell'esercizio delle proprie funzioni, è indipendente rispetto alle funzioni operative.

Il DPO è dotato delle risorse umane e finanziarie necessarie all'adempimento dei suoi compiti.

Il DPO è nominato formalmente dal Titolare e la nomina è comunicata all'Autorità di Controllo.

Compiti principali del DPO sono:

1. informare e fornire consulenza al Titolare (e/o al Soggetto Delegato, o al Referente privacy, o in genere alle funzioni coinvolte nel trattamento dei dati o nelle questioni conseguenti) in merito agli obblighi derivanti dalla Normativa;
2. verificare che le politiche del Titolare o dei Responsabili Esterni in materia di protezione dei Dati siano conformi alla normativa vigente e correttamente attuate;
3. fornire pareri in merito alla valutazione d'impatto sulla protezione dei Dati (DPIA) e sorvegliare i relativi adempimenti;
4. fungere da punto di contatto per gli Interessati in merito a qualunque problematica connessa al trattamento dei Dati, o all'esercizio dei loro diritti;
5. mantenere i contatti con l'Autorità;
6. monitorare lo stato delle nomine in ambito privacy e, qualora necessario, attivare le funzioni preposte per gli opportuni aggiornamenti;
7. sovrintendere alla formazione del personale;
8. monitorare i trattamenti inseriti nel registro dei trattamenti e il suo corretto aggiornamento.

6.4 Referente Privacy

Il Referente Privacy ha il compito di sovrintendere ai processi ed agli adempimenti in materia di Privacy, in collaborazione con il DPO e con ogni altra funzione cui siano attribuite, in via continuativa o transitoria, mansioni e/o obbligazioni relative (o connesse) alla regolazione Privacy.

Si occupa dell'applicazione della normativa sulla sicurezza dei Dati nei contesti operativi delle Società del Gruppo e, in tal senso, supporta i Titolari (e/o il/i Soggetto/i Delegato/i ed il/i DPO).

Compiti principali del Referente Privacy sono:

1. coordinare le esigenze informatiche (ambienti e accessi) del personale del Gruppo Ascopiave;
2. fornire consulenza ed assistenza operativa agli addetti delle Società del Gruppo su

problematiche inerenti temi Privacy;

3. curare la tenuta e l'aggiornamento del Registro dei Trattamenti, con frequenza almeno semestralmente e comunque ogni volta si verifichino variazioni di elementi rilevanti (nuovo trattamento, modifica della normativa di riferimento e/o delle modalità di trattamento, etc.);
4. curare la tenuta e l'aggiornamento dell'elenco delle banche dati, sia informatizzate che cartacee, gestite e custodite a livello di Gruppo;
5. curare l'aggiornamento semestrale dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
6. gestire, con la supervisione del DPO, le attività di formazione del personale in ambito Privacy, con particolare riguardo ai nuovi assunti.

6.5 Persona autorizzata al trattamento dei dati personali (o “Autorizzato”, o “Incaricato”)

La figura della “Persona autorizzata al trattamento dei dati personali” non ha una definizione propria nella Normativa. Tuttavia, la stessa può essere assimilata a quella dell’“Incaricato al trattamento” di cui alla regolazione vigente prima del GDPR.

In conseguenza, sono “Autorizzati” (o Incaricati) al trattamento tutti i dipendenti o collaboratori delle Società del Gruppo (Titolari o Responsabili del trattamento) che, nel normale esercizio delle proprie mansioni, sono chiamati a trattare i Dati.

Ad ognuno, il Titolare (o il Responsabile) conferisce specifiche “Istruzioni per il trattamento dei dati personali”, mediante apposito atto scritto.

Tra gli Incaricati anzidetti, si distinguono, per posizione gerarchica e responsabilità, i “Focal Point”, di cui al successivo paragrafo 6.6.

Nello svolgimento delle proprie attività, gli Incaricati, oltre a quanto precisato nelle Istruzioni per il trattamento (su citate), si attengono alle disposizioni del presente documento e sono soggetti al vincolo di riservatezza. In particolare, ognuno deve mantenere strettamente riservati e confidenziali i Dati che abbia a trattare, quindi non deve:

1. divulgarli, con qualunque mezzo, al di fuori della compagine aziendale, o comunque a persone non autorizzate a trattarli, salva la sussistenza di eventuali espliciti obblighi normativi in tal senso ^[1];
2. lasciare incustoditi, nemmeno per brevi periodi:
 - a) documenti contenenti i Dati;

¹ Resta fermo ed impregiudicato il rispetto della disciplina “Unbundling”, di cui alla Delibera AEEGSI n. 296/2015/R/com (Testo Integrato Unbundling Funzionale - TIUF) e s.m.i., con rigorosa osservanza del “Codice di Comportamento del personale coinvolto nelle attività separate funzionalmente”, presente nella sezione dedicata del sito internet delle Società del Gruppo.

b) computer, tablet, smartphone o similari, senza preventivo inserimento del blocco all'accesso;

c) password di accesso agli apparati di cui alla lett. b, o ai sistemi gestionali o informatici.

Inoltre, ogni Incaricato al trattamento, al fine di preservare i Dati personali, è tenuto ad osservare le seguenti linee guida comportamentali:

1. accedere ai Dati utilizzando unicamente il proprio profilo autorizzativo;
2. operare in modo che siano ridotti al minimo i rischi di distruzione e/o perdita anche accidentale dei Dati;
3. chiudere (o sospendere) la sessione di lavoro prima di allontanarsi dal proprio pc, o dispositivo mobile (tablet o telefono), evitando di lasciare documenti in vista;
4. non salvare documenti contenenti Dati personali sul proprio pc e/o su dispositivo rimovibile, ovvero nella memoria del dispositivo mobile (tablet o telefono);
5. ove autorizzato al lavoro "da casa" o "da remoto", accedere ai file di lavoro solo dopo aver accertato l'adeguatezza del pc (o altro apparato), della linea e dei sistemi antivirus ed anti-intrusione a garantire la sicurezza dei Dati personali trattati;
6. avere la diligente custodia dei dispositivi a proprio uso esclusivo, impedendo l'utilizzo dei medesimi da parte di terzi estranei alla compagine aziendale, o comunque non legittimati ad accedere ai Dati;
7. avvalersi esclusivamente di soggetti abilitati per la risoluzione di problematiche tecniche che potrebbero comportare il rischio di cancellazione, danneggiamento e/o diffusione/dispersione dei Dati personali trattati;
8. distruggere i documenti e/o le copie dei documenti, quando questi non siano più necessari per l'attività dell'Incaricato;
9. alla fine della giornata lavorativa:
 - liberare la propria postazione, riponendo qualsiasi documento contenente Dati personali, all'interno dei propri raccoglitori, cassette e/o armadi;
 - effettuare il log off e spegnere il proprio pc;
10. informare tempestivamente, o segnalare al Focal Point di riferimento (o alla Funzione Privacy, o al DPO):
 - di ogni richiesta o reclamo che avesse a pervenire da uno o più Interessati, o dall'Autorità di controllo e/o dall'Autorità Giudiziaria, di cui dovesse avere notizia;
 - di ogni situazione di pericolo, anche solo potenziale, di cancellazione, danneggiamento, accesso o divulgazione non autorizzati o illeciti di cui venisse a conoscenza;
 - di ogni situazione in cui, accidentalmente, avesse a venire in possesso, o comunque ad accedere a Dati personali ulteriori rispetto a quelli connessi allo svolgimento della propria mansione, mantenendo l'assoluto riserbo su tali Dati;
 - di ogni dubbio in merito alla liceità di Trattamenti e/o alle concrete modalità di

trattamento consentite e/o da adottarsi;

- di ogni ulteriore anomalia o casistica rilevante nell'ambito della protezione dei Dati personali che avesse a riscontrare;
- nell'eventualità, della (ritenuta) esigenza di avviare un nuovo Trattamento, ovvero di modificare o integrare le finalità di un Trattamento già in essere, ovvero di nominare uno o più Responsabili al trattamento;

11. ove il Trattamento avesse come base giuridica l'espresso consenso degli Interessati (quale, ad esempio, il Trattamento a fini di marketing e/o profilazione di cui al successivo paragrafo 9), attenersi scrupolosamente alle finalità ed ai limiti espressi con il consenso medesimo, astenendosi da qualsivoglia Trattamento ulteriore o diverso;

12. non comunicare Dati personali a soggetti terzi, estranei alla compagine aziendale, salva preventiva verifica della loro legittimazione in tal senso (es. mediante l'avvenuta nomina a Responsabili al Trattamento);

La mancata osservanza delle obbligazioni di cui sopra, come anche, più in generale, di quanto previsto dalla Normativa, dalla presente Policy e dai documenti connessi, è fonte di responsabilità disciplinare (e/o negoziale), salva ed impregiudicata ogni altra sanzione prevista dalla legge.

6.6 Focal Point

Il Titolare nomina i Focal Point, per il trattamento dei Dati dell'area di rispettiva competenza, tramite apposito atto contenente specifiche istruzioni.

I Focal Point collaborano con la Funzione Privacy nell'ambito delle tematiche oggetto del presente documento.

In particolare, ai Focal Point, in virtù della peculiare posizione nell'organizzazione aziendale, in aggiunta ai generali obblighi propri degli Autorizzati al trattamento, oltre agli obblighi propri di ogni Incaricato al trattamento di cui al precedente paragrafo 6.5, sono assegnate le seguenti responsabilità:

- segnalare alla Funzione Privacy l'opportunità o l'esigenza di migliorare o implementare ulteriori misure di sicurezza sui trattamenti di propria competenza;
- vigilare e controllare che le attività di trattamento, in capo agli Incaricati appartenenti all'area di competenza, si svolgano nel rispetto della regolazione e delle Policy aziendali, garantendo altresì che gli stessi rispettino rigorosamente gli obblighi di riservatezza;
- effettuare i controlli necessari per accertare che i Dati personali siano trattati nel rispetto dei diritti e dei principi fissati dalla Normativa;
- collaborare con la Funzione Privacy;
- avvisare, in via preventiva, la Funzione Privacy in caso di:
 - progetti che prevedano nuovi trattamenti di Dati personali, o modifiche significative a trattamenti già in essere;

- stipula di atti che determinino l'esigenza di provvedere alla nomina (o all'accettazione della nomina) di Responsabile del trattamento (o la definizione di un accordo di contitolarità);
- segnalare tempestivamente alla Funzione Privacy la ricezione di eventuali richieste o domande che avessero a pervenire dagli Interessati al trattamento, ai sensi degli art. da 15 a 22 del Regolamento;
- informare prontamente la Funzione Privacy di tutte le questioni rilevanti ai sensi del Regolamento (ad esempio richieste del Garante, esiti delle ispezioni delle Autorità, ecc.).

I Focal Point hanno altresì l'obbligo di dare immediata segnalazione alla Funzione Privacy di ogni violazione delle norme di Legge o dei Regolamenti interni che dovessero riscontrare, nonché di ogni violazione dei dati personali ("Data Breach" – rif. art. 34 del Regolamento) di cui avessero notizia.

6.7 Funzione Privacy

L'organismo ha, in generale, una funzione di assistenza e consulenza sulle questioni Privacy nei confronti di tutti i soggetti incaricati dei trattamenti. Inoltre, ha la responsabilità specifica di garantire la gestione delle segnalazioni di violazione di Dati personali.

6.8 Responsabili esterni del trattamento dei dati personali

La nomina a Responsabile del trattamento è obbligatoria quando un soggetto (persona fisica o giuridica), estraneo all'organizzazione aziendale del Titolare, svolga, a favore di quest'ultimo, attività, mansioni o compiti da cui derivi o consegua l'esigenza di trattare Dati personali già in capo al Titolare.

La nomina avviene tramite un apposito atto scritto che specifichi: la finalità perseguita, la tipologia dei Dati, la durata del trattamento e gli obblighi del Responsabile del trattamento, oltre alle concrete modalità di trattamento.

Il Titolare, per il tramite delle figure aziendali competenti, vigila sulla puntuale osservanza delle disposizioni in materia di trattamento dei Dati fissate nell'atto di nomina.

Il Responsabile del trattamento può, a sua volta, nominare un sub-responsabile solo previa e specifica autorizzazione in tal senso del Titolare.

6.9 Amministratore di Sistema

Gli Amministratori di sistema sono nominati dal Titolare mediante specifica lettera di incarico.

Gli Amministratori di sistema possono essere interni, cioè individuati tra i dipendenti delle Società del Gruppo, o esterni, cioè individuati tra le persone fisiche alle quali Ascopiave (o altra Società del Gruppo) ha deciso di affidare la gestione dei sistemi informativi.

Copia del/degli atto/i di nomina è inoltrata al DPO.

Ferme restando le responsabilità previste dalla Normativa, di seguito si riportano le principali

responsabilità proprie di ogni Amministratore di sistema:

- vigilare sul corretto utilizzo dei sistemi informatici;
- gestire, d'intesa con le direzioni interessate, il processo di autenticazione / abilitazione per l'accesso alle banche dati personali informatiche;
- preservare le informazioni aziendali, attraverso attività di backup o disaster recovery, organizzazione dei flussi di rete, gestione dei supporti di memorizzazione o manutenzione hardware, ecc.;
- assicurare la custodia e l'integrità delle componenti riservate delle credenziali di autenticazione;
- segnalare alla Funzione Privacy ogni criticità che avessero a rinvenire nell'ambito della gestione dei Dati personali, con particolare, ma non esclusivo riguardo alle ipotesi di Data Breach.

6.10 Amministratore dei sistemi di videosorveglianza

L'Amministratore dei sistemi di videosorveglianza è nominato dal Titolare (o dal Soggetto Delegato), mediante specifica lettera di incarico.

La nomina è obbligatoria per ciascuna Società del Gruppo che sia proprietaria o conduttrice di immobili e/o di aree soggette a videosorveglianza.

Copia del/degli atto/i di nomina è inoltrata al DPO.

Le responsabilità dell'Amministratore dei sistemi di videosorveglianza sono analoghe a quelle in capo agli amministratori di sistema (pur se limitate alle tematiche proprie della videosorveglianza) e sono elencate, con precisione, nel Provvedimento in materia di Videosorveglianza emanato dal Garante della Protezione dei Dati Personali l'8 Aprile 2010 (che si richiama integralmente), nonché nel Regolamento aziendale sulla videosorveglianza, salvo ed impregiudicato quanto ulteriormente previsto dall'Autorità di controllo.

In particolare, l'Amministratore dei sistemi di videosorveglianza deve assicurarsi che l'utilizzo degli impianti di videosorveglianza da parte delle persone autorizzate avvenga nel rispetto dei principi applicabili al trattamento dei Dati ed esclusivamente per finalità determinate, esplicite e legittime.

7. Diritti dell'interessato

Il Titolare, riconosce e garantisce agli Interessati l'esercizio dei diritti riconosciuti a questi ultimi, in conformità con quanto stabilito e richiesto dalla Normativa. In particolare, ogni Interessato, ha diritto:

1. di accesso, ovvero di ottenere dal Titolare, o Contitolare (o dal Responsabile del trattamento) la conferma che sia o meno in corso un trattamento di propri Dati appartenenti e, in tal caso, ottenere l'accesso ai Dati medesimi;
2. di rettifica, cioè ad ottenere, senza ingiustificato ritardo, la rettifica dei propri Dati che abbiano

ad essere inesatti e/o incompleti;

3. di opposizione, cioè di opporsi, in qualsiasi momento al trattamento dei propri Dati. Il Titolare, in dette circostanze, può continuare il trattamento solo nel caso in cui, in tal senso, a favore del Titolare, sussistano motivi legittimi prevalenti su quelli dell'Interessato (es. tutela giudiziale di un diritto del Titolare);
4. alla cancellazione, dei propri Dati senza ingiustificato ritardo, qualora i Dati:
 - siano trattati illecitamente;
 - debbano essere cancellati in virtù di un obbligo legale cui sia soggetto il Titolare;
 - non siano più necessari, in relazione alle finalità per i quali sono stati raccolti e/o trattati;
 - rispetto ai quali il consenso su cui si basa il trattamento sia stato revocato, oppure pervenga l'opposizione al trattamento da parte dell'Interessato e non sussistano altri fondamenti giuridici che consentano di mantenere il trattamento;
5. alla limitazione del trattamento, quando:
 - l'accuratezza dei Dati è contestata o l'Interessato si è opposto al loro trattamento, per il periodo necessario allo svolgimento delle verifiche in merito all'esattezza dei Dati o all'eventuale prevalenza dei motivi legittimi che consentano al Titolare di mantenere il trattamento, nonostante l'opposizione;
 - il trattamento è illecito, ma l'Interessato si è opposto alla cancellazione dei Dati, chiedendo che ne sia limitato l'utilizzo;
 - i Dati siano necessari all'Interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
6. alla portabilità dei Dati, ovvero a ricevere, in un formato strutturato, di uso comune e leggibile da dispositivo automatico i propri Dati, nonché (qualora il trattamento sia basato sul consenso, sia effettuato con strumenti automatizzati ed ove tecnicamente fattibile) a trasmettere gli stessi ad altro Titolare senza impedimenti;
7. di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che abbia a produrre effetti giuridici in capo all'Interessato o che incida significativamente sulla sua persona;
8. di essere informato laddove una richiesta relativa all'esercizio dei propri diritti sia stata, o debba essere, rigettata, con esplicitazione delle relative motivazioni.

Si rimanda a quanto precisato nella "Policy gestione diritti degli interessati" che disciplina, nel dettaglio, le modalità di esercizio dei Diritti degli interessati.

8. Adempimenti generali per il trattamento dei dati personali

8.1 Informative

Prima e/o contestualmente all'avvio del trattamento, il Titolare deve sempre rilasciare un'apposita Informativa all'Interessato, che contiene, essenzialmente:

- le finalità del trattamento e la base giuridica dello stesso;
- la tipologia dei Dati oggetto del trattamento;
- l'identità ed dati di contatto del Titolare;
- i dati del contatto del DPO;
- il periodo di conservazione dei Dati, o i criteri utilizzati per determinare tale periodo;
- i diritti dell'Interessato.

Qualora il Titolare intenda trattare i Dati personali per una finalità diversa e/o ulteriore rispetto a quella per cui essi sono stati raccolti, si impone, in via preventiva, il rinnovo dell'Informativa. Questa dovrà dar conto della diversa/ulteriore finalità, unitamente ad ogni informazione pertinente.

8.2 Base giuridica del trattamento

Il trattamento dei Dati deve disporre di una base giuridica legittima.

Questa si riscontra quando l'Interessato ha prestato il proprio consenso, in conformità alle condizioni di cui all'art. 7 del Regolamento e quando il Trattamento è necessario:

- a) all'esecuzione di un contratto di cui l'Interessato è parte, o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- b) per adempiere a un obbligo legale a cui è soggetto il Titolare;
- c) per la salvaguardia degli interessi vitali dell'Interessato, o di un'altra persona fisica;
- d) per l'esecuzione di un compito di interesse pubblico, o per l'esercizio di pubblici poteri conferiti al Titolare;
- e) ai fini degli interessi legittimi perseguiti dal Titolare, o da una terza parte, qualora questi siano tali da superare gli interessi o i diritti dell'Interessato.

Nelle ipotesi di cui alle lettere da "a" ad "e", in consenso esplicito dell'Interessato non è essenziale, fermo l'obbligo di informativa ai sensi del punto 8.1 ed il rispetto di quanto previsto ai punti che seguono.

8.3 Finalità previste

I Dati devono essere raccolti per finalità determinate, esplicite e legittime, quindi trattati secondo modalità compatibili con tali finalità.

I Dati non devono essere utilizzati in modo contrario agli scopi previsti e comunicati attraverso l'Informativa.

Successivamente al conseguimento delle finalità previste dal Trattamento, conformemente a

quanto previsto dall'art. 89, paragrafo 1 del GDPR, la conservazione dei Dati, di norma, è ammessa unicamente per scopi di archiviazione nell'interesse pubblico, ricerca scientifica o storica o esigenze statistiche.

8.4 Riservatezza del trattamento dei dati e loro classificazione

Ai soggetti che trattano i Dati è fatto assoluto vietato utilizzare gli stessi per i propri scopi privati e/o renderli accessibili a qualsiasi soggetto non autorizzato, quindi al di fuori delle casistiche previste dalla normativa.

I divieti anzidetti si estendono anche all'ipotesi in cui si configuri l'accesso accidentale ai Dati da parte di dipendenti Ascopiave (e/o delle Società del Gruppo) che non abbiano necessità di accedervi per l'espletamento delle relative mansioni. Agli stessi, al pari dei legittimati, si impone, in ogni caso (il connesso) obbligo di riservatezza.

8.5 Categorie particolari di Dati personali

Il Trattamento dei Dati Particolari di cui all'art. 9 del Regolamento (ex "dati sensibili") è consentito solo nei termini stabiliti dalla Normativa. In sintesi, ciò si verifica esclusivamente quando l'Interessato ha prestato il proprio consenso esplicito riferito a tali dati, per una o più finalità specifiche, ovvero, per quanto qui rileva, quando il Trattamento:

- è necessario ai fini dello svolgimento degli obblighi e/o dell'esercizio di specifici diritti del Titolare, o dell'Interessato, in materia di diritto del lavoro, della sicurezza e protezione sociale, nella misura e nei limiti in cui lo stesso sia autorizzato dal diritto comunitario, o nazionale, o da un contratto collettivo e vengano predisposte garanzie appropriate per i diritti fondamentali e gli interessi dell'Interessato;
- è necessario per proteggere gli interessi vitali, dell'Interessato o di un'altra persona fisica, qualora l'Interessato sia fisicamente o giuridicamente incapace di prestare il proprio consenso;
- si riferisce a Dati personali che siano manifestamente resi pubblici dall'Interessato;
- è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria, o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
- è necessario ai fini della medicina preventiva o occupazionale, per la valutazione della capacità lavorativa del dipendente sulla base della legislazione comunitaria, nazionale o negoziale con un operatore sanitario (es. Medico competente ai sensi del D.Lgs. 81/2008 e s.m.i.).

Ai sensi dell'art. 10 del GDPR, i Dati relativi alle condanne penali ed ai reati costituiscono una peculiare categoria di Dati Particolari, applicandosi quindi agli stessi la medesima disciplina di cui sopra. In particolare, in dette circostanze, il Trattamento può/deve avvenire:

- sotto il controllo dell'Autorità pubblica o

- solo nel caso in cui questo sia autorizzato dal diritto comunitario o nazionale, ferma l'adozione di garanzie appropriate per i diritti e le libertà degli Interessati.

A seconda della categoria di Dati e dei conseguenti rischi associati al Trattamento, Ascopiave e le Società del Gruppo adottano (e/o adotteranno) le misure di sicurezza adeguate a garantire la tutela dei diritti e delle libertà degli Interessati (ad esempio, pseudonimizzazione, dispositivi di sicurezza tecnica, crittografia e limitazione dell'accesso fisico).

8.6 Registro dei trattamenti

Il Referente Privacy, con l'eventuale supporto della Funzione Privacy (e l'ausilio, in termini di debita e tempestiva informativa dei Focal Point, in ordine alle eventuali esigenze di implementazione e/o modifica), provvede alla costituzione, alla regolare tenuta ed all'aggiornamento del Registro delle Attività di Trattamento eseguite dagli Incaricati e dai Responsabili Esterni.

Il Registro contiene le seguenti informazioni:

- la tipologia dei Dati trattati nei diversi Trattamenti;
- le finalità del Trattamento;
- la descrizione delle categorie di Interessati;
- il formato (elettronico e/o cartaceo) dei Dati trattati;
- i dati di contatto del Titolare, del DPO e (nell'eventualità) del Responsabile al trattamento;
- le strutture aziendali (delle Società del Gruppo) coinvolte nel Trattamento;
- le categorie di destinatari a cui sono stati, verranno o potranno essere divulgati i Dati;
- i sistemi applicativi di riferimento;
- la descrizione degli archivi fisici;
- ove possibile, i termini previsti per la cancellazione delle diverse categorie di Dati ed una descrizione generale delle misure tecniche e organizzative di sicurezza adottate e da adottarsi.

I singoli Focal Point, anche al fine di consentire la corretta tenuta e l'aggiornamento del Registro delle Attività di Trattamento, consultata eventualmente la Funzione Privacy, segnalano al Referente Privacy, con la massima celerità, gli eventuali ulteriori Trattamenti e/o l'avvenuta nomina a Responsabile al trattamento in capo a Società del Gruppo e/o l'avvenuta nomina di nuovi Responsabili al trattamento da parte della Società del Gruppo e/o l'intervenuta modifica di Trattamenti esistenti.

In dette circostanze, i Focal Point trasmettono altresì al Referente Privacy la documentazione a supporto (es. copia degli atti da cui derivano le esigenze anzidette, testo delle Informative impiegate, atti di nomina a/della Società del Gruppo a Responsabile al trattamento, ecc.).

8.7 Data Breach e flussi comunicativi all’Autorità

Tutti gli Incaricati, nonché, in genere, tutti i soggetti in qualunque modo coinvolti nel Trattamento di Dati hanno l’obbligo di segnalare, con la massima celerità e comunque senza indugio, anzitutto al Focal Point di riferimento (ma, nel caso, anche direttamente al DPO o alla Funzione Privacy), ogni violazione, o sospetta violazione dei Dati, come la distruzione, la perdita, la divulgazione, l’accesso non autorizzato o l’alterazione di Dati trattati, dovuta sia a cause accidentali che quale conseguenza di azioni illecite (“Data Breach”).

Il Focal Point che ritenga verificata una situazione di violazione dei Dati, ovvero che abbia a ricevere la segnalazione di cui al comma 1, informa immediatamente la Funzione Privacy per i necessari approfondimenti e le azioni eventualmente conseguenti.

Il Titolare, con il supporto della Funzione Privacy e la collaborazione dei Focal Point, degli Amministratori di sistema e/o degli Amministratori di videosorveglianza, nonché di ogni altra risorsa ritenuta necessaria o utile, mette in atto le misure necessarie per l’individuazione ed il contenimento delle violazioni dei Dati che avessero ad essere effettivamente individuate. Nei casi previsti dalla Normativa e nel rispetto delle relative modalità e tempistiche, normalmente per il tramite del DPO, assicura altresì la debita segnalazione all’Autorità ed agli Interessati.

Il Referente Privacy, ai sensi dell’articolo 33, comma 5 del Regolamento, tiene traccia in un apposito registro di tutti gli incidenti, compresi quelli per i quali non sussiste obbligo di notifica.

Si rimanda a quanto precisato nel documento “Ascopiave_GDPR_Data Breach Procedure”, che disciplina, nel dettaglio, le modalità di gestione delle situazioni di violazione dei Dati personali.

8.8 Data Protection Impact Assessment e misure di sicurezza

Il Titolare, nei casi e secondo le modalità previste dalla Normativa, assicura che, prima di procedere ad un nuovo Trattamento (e/o prima di attuare modifiche significative su un Trattamento, in ipotesi, già in essere), venga effettuata una valutazione d’impatto sulla protezione dei Dati (Data Protection Impact Assessment).

A tale scopo, ogni Focal Point è tenuto a monitorare i Trattamenti in essere e/o da avviare nella propria area di competenza, quindi a segnalare, al DPO o alla Funzione Privacy, ogni situazione in cui possa rendersi necessaria l’espletamento di una valutazione di impatto. Nel dubbio, i Focal Point possono valersi dell’assistenza / consulenza della Funzione Privacy.

All’esito delle valutazioni (nei casi in cui queste si rendono necessarie, ai sensi della Normativa), alla luce dei risultati di queste, il Titolare adotta le misure più appropriate per ridurre il livello di rischio, quindi per proteggere i Dati da modifiche, cancellazioni o perdite non autorizzate. A titolo esemplificativo e non esaustivo, queste possono consistere in:

- pseudonimizzazione, minimizzazione e cifratura dei Dati;
- strumenti e procedure operative tali da assicurare la riservatezza, l’integrità, la disponibilità e la resilienza dei sistemi e dei servizi che trattano i Dati;

- strumenti e modalità per ripristinare tempestivamente la disponibilità e l'accesso ai Dati in caso di incidente fisico o tecnico;
- processi per testare l'efficacia delle misure tecniche e organizzative volte a garantire la sicurezza del Trattamento.

Qualora la valutazione d'impatto indichi che il Trattamento, nonostante l'adozione delle misure di cui al comma precedente, presenta un rischio elevato per i diritti e le libertà degli Interessati, ai sensi dell'art. 36 del Regolamento, il Titolare, sentito il DPO, prima di procedere al relativo Trattamento, consulta l'Autorità di controllo.

Si rimanda a quanto precisato nel documento "Ascopiave_GDPR_Metodologia DPIA", che disciplina, nel dettaglio, la metodologia di Data Protection Impact Assessment.

8.9 Formazione

Il Titolare assicura a tutti gli Incaricati al trattamento ed in genere al personale dipendente, una formazione adeguata rispetto alla Normativa ed alla conseguenti Policy, Procedure e/o regole di condotta.

L'effettivo svolgimento della formazione e della sensibilizzazione in merito alle tematiche relative alla protezione dei Dati è monitorato dal DPO e curato dalla Funzione Privacy.

8.10 Trasferimento di dati personali

Premettendo che, nel contesto operativo del Gruppo Ascopiave, trattasi situazione oltremodo eccezionale e/o assolutamente marginale, il trasferimento di Dati oltre i confini dell'Unione Europea è consentito solo se nel Paese di destinazione viene garantito un livello di protezione adeguato a quello conseguente alla Normativa europea.

Il trasferimento dei Dati, salva l'esigenza di esplicita (preventiva) indicazione nell'ambito della relativa Informativa agli Interessati, deve essere autorizzato esplicitamente dal Titolare, sentito il DPO.

8.11 Cooperazione con l'Autorità di controllo – Gestione delle istanze in materia di Privacy

Il Gruppo Ascopiave assicura e persegue l'obiettivo della massima collaborazione con l'Autorità di controllo (in Italia il "Garante per la Protezione dei Dati Personali) e, più in generale, con gli Enti e le Istituzioni preposte alla tutela della salvaguardia dei Dati personali.

Ai sensi della normativa, il primo referente dell'Autorità è il DPO.

Nel contesto del Gruppo, allo stesso, si affianca l'intera Funzione Privacy.

I Focal Point ed in genere tutti gli Incaricati e qualunque dipendente devono cooperare con il DPO e la Funzione Privacy per consentire e rendere concreta la collaborazione anzidetta e l'interlocuzione con l'Autorità, anche e soprattutto nell'ambito delle indagini che questa avesse ad

avviare, nonché per permettere la corretta e compiuta gestione delle richieste e/o dei reclami che avessero a pervenire dagli Interessati. In particolare, a fronte dell'istanza del DPO (e/o della Funzione Privacy nel suo complesso), è fatto obbligo ad ogni dipendente di fornire, nei limiti delle proprie competenze e conoscenze, diretto e veritiero riscontro, senza necessità di ottenere il vaglio, l'autorizzazione o nulla osta che dir si voglia dal proprio responsabile o superiore gerarchico.

In presenza di richieste, reclami e/o contestazioni in materia di Privacy, che pervengano da un Interessato, dall'Autorità e/o da ogni altro Ente preposto, il soggetto ricevente è tenuto a darne tempestiva comunicazione al Focal Point di riferimento, il quale, a sua volta, informa immediatamente il DPO o la Funzione Privacy, fornendo ogni informazione utile alla successiva gestione.

8.12 Monitoraggio della conformità

Il Titolare garantisce un continuo monitoraggio in merito alla corretta applicazione della Normativa, della presente e della disciplina interna in materia di Privacy, disponendo gli interventi correttivi ritenuti necessari, da attuare anche per il tramite dei Responsabili del trattamento.

Nell'ambito del Gruppo, il Soggetto Delegato di Ascopiave assicura un'adeguata attività di reporting al Consiglio di Amministrazione della medesima capo-gruppo, in merito a quanto sopra.

Nel caso si rendano necessarie modifiche alla citata disciplina interna dovute a sopravvenute disposizioni di legge e/o provvedimenti cogenti, queste potranno essere adottate dal Soggetto Delegato di Ascopiave, sentito il DPO, senza necessità di preventiva approvazione da parte del Consiglio di Amministrazione.

9. Attività peculiari - Marketing e Profilazione

Nell'ambito dei diversi, possibili Trattamenti che le Società del Gruppo potrebbero astrattamente porre in essere, una peculiare attenzione debba riferirsi a quelli da avviarsi per finalità di Marketing e/o Profilazione.

Rispetto a questi, il Titolare deve sempre, obbligatoriamente, acquisire dall'Interessato, evidentemente in via preventiva, un consenso specifico, separato, espresso e documentato. La prestazione del consenso medesimo è, in ogni caso, facoltativa, oltrechè revocabile in ogni momento dall'Interessato, senza pregiudizio per i rapporti negoziali eventualmente instaurati.

Mediante il conferimento del consenso (ai sensi dell'art. 6, comma 1, lettera a) del Regolamento) l'Interessato prende specificatamente atto delle finalità promozionali, commerciali, di marketing e/o di profilazione del Trattamento (incluse le attività gestionali e amministrative conseguenti) e, prestando il consenso, autorizza espressamente il Trattamento ai sensi della Normativa.

L'Interessato, inoltre, resta in ogni caso libero:

- a. di prestare, o negare il consenso all'ulteriore comunicazione a soggetti terzi che, a loro volta, vogliono procedere al Trattamento per finalità di marketing e/o profilazione. Laddove l'Interessato neghi detto ultimo consenso, Ascopiave (o qualunque altra Società del Gruppo) non effettuerà alcuna comunicazione a soggetti terzi, mentre i Dati (sul presupposto dell'ottenimento del consenso di cui al comma 2) saranno trattati solo ed esclusivamente dalla/e Società del Gruppo che ha/hanno ottenuto il consenso medesimo;
- b. di prestare il consenso al trattamento per finalità di marketing e di non prestarlo per la profilazione (e/o per la comunicazione a terzi che vogliono a loro volta procedere al trattamento per finalità di profilazione, applicandosi conseguentemente quanto sancito dalla precedente lett. a)

Nell'ambito di una rigorosa applicazione della Normativa ed al fine di garantire la massima tutela dei diritti degli Interessati, le Società del Gruppo, prima di avviare un nuovo trattamento per finalità di marketing e/o profilazione, provvedono, per il tramite del/dei Focal Point di riferimento, a:

- 1) pre-avvisare la Funzione Privacy;
- 2) svolgere, con l'ausilio della medesima Funzione Privacy, la valutazione d'impatto sulla protezione dei Dati (Data Protection Impact Assessment) ai sensi del paragrafo 8.8 e di quanto previsto nel documento "Ascopiave_GDPR_Metodologia DPIA".

Ogni Società del Gruppo interessata, quale Titolare (o con-titolare, o Responsabile) del Trattamento, sarà poi tenuta ad adottare le misure necessarie a ridurre ed a mantenere il livello di rischio entro il limite definito in sede di DPIA.