ASCO HOLDING

Privacy Policy

Adottata il 18 gennaio 2021

Ultimo aggiornamento del 1 luglio 2021

Indice

1. Premessa

Asco Holding S.p.A., con sede legale in Pieve di Soligo (TV), via Verizzo 1030 (di seguito "**Asco Holding**") si occupa della gestione delle partecipazioni societarie. Tra queste, la più rilevante è quella in Ascopiave S.p.A., società quotata alla Borsa valori di Milano (cui si aggiungono le partecipazioni in BIM Piave Nuove Energie S.R.L. ed Asco TLC S.p.A.).

Asco Holding, conseguentemente, tratta essenzialmente Dati personali presenti in pubblici registri, o destinati a diventare di dominio pubblico (es. referenti dei soci, amministratori e sindaci delle società partecipate, ecc.). Anche dal punto di vista quantitativo, il volume dei Dati personali risulta estremamente limitato. La Società, pertanto, non è soggetta all'obbligo di nomina del Responsabile della Protezione dei Dati.

Asco Holding ha stipulato un contratto di servizio con la controllata Ascopiave che, tra l'altro, prevede la fornitura del servizio di gestione degli adempimenti Privacy. In ragione di detto rapporto negoziale, Asco Holding si avvale e può avvalersi delle seguenti figure di Ascopiave (le cui funzioni saranno precisate nel prosieguo del presente documento): la Funzione ed il Referente Privacy, gli Amministratori di Sistema, gli Amministratori di videosorveglianza ed eventualmente i Focal Point.

In caso di recesso o di cessazione per altra causa del menzionato contratto di servizio, Asco Holding provvederà autonomamente agli adempimenti Privacy, individuando all'interno della propria struttura le necessarie figure ed apportando le dovute modifiche e/o integrazioni alla presente Policy.

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 di quei 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, ad esempio, 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 in genere tutti coloro che svolgono un'attività che comporti delle relazioni con soggetti fisici dovranno attenersi a quanto previsto dalla normativa di cui sopra.

Asco Holding, alla luce di quanto precisato in premessa, dunque della limitatezza dei Trattamenti svolti, ha ritenuto di adottare un'unica Privacy Policy, disciplinante tutte le tematiche rilevanti in materia di protezione dei Dati personali.

I dipendenti di Asco Holding, che trattino Dati personali in ragione delle funzioni aziendali svolte, sono tenuti a seguire la citata disciplina sulla protezione dei Dati personali attenendosi alla presente Privacy Policy (o "Manuale").

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 necessari 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 relativo 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";
- 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 Asco Holding 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, nel presente Manuale saranno altresì trattate, in appositi paragrafi, le seguenti tematiche:

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 [1] 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 abbiano 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, Asco Holding è tenuta ad assicurare la protezione dei Dati trattati nell'ambito della propria attività.
A tal fine Asco Holding 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 entri in possesso.
Alla luce di quanto sopra, Asco Holding 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:

[1] Il principio dell'Accountability impone al Titolare del Trattamento di mettere in atto misure tecniche e organizzative adeguate a garantire (ed essere in grado di dimostrare) che il Trattamento sia effettuato conformemente al GDPR. Dette misure devono essere riesaminate ed aggiornate, qualora necessario.

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 devo 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, vanno aggiornati adottandosi 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 garantirne un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da Trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione e/o dal danno accidentale.

5. Definizioni

Ai fini del presente Manuale e, in genere, per le tematiche proprie o connesse 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 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. Ai fini della presente Policy, agli Amministratori di Sistema, propriamente intesi, sono assimilati gli Amministratori di data base.
Amministratore dei sistemi di	Persona fisica addetta alla gestione operativa degli impianti

videosorveglianza	di videosorveglianza, nel rispetto dei principi applicabili al Trattamento dei Dati personali di cui all'art.5 del GDPR.
Amministratore dei sistemi di videosorveglianza con funzioni di responsabilità	Persona fisica responsabile di sovraintendere alla 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")**	È 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 **(o Violazione di Dati personali)**	Ogni evento che comporta, accidentalmente o in modo 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 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.
Focal Point	Soggetti eventualmente designati (e nominati), in ragione del loro ruolo strategico nell'ambito dell'organizzazione aziendale, con il compito di sovraintendere ai progetti ed alle attività societarie che abbiano e/o possano avere incidenza sul Trattamento di Dati personali. 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).
Funzione Privacy	È un organismo designato da Ascopiave, che ha, quali componenti stabili, il Soggetto Delegato ed il DPO di Ascopiave, nonché 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. A seconda delle esigenze, la compagine può essere integrata da altre funzioni (es. Direzioni Legal e ICT, Focal Point, ecc.). L'organismo ha altresì la responsabilità specifica di garantire la gestione delle segnalazioni di violazione di Dati personali (Data Breach).
GDPR **(o Regolamento)**	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.
Misure di sicurezza	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 Trattamenti. Ascopiave, anche per conto di Asco Holding, ha predisposto un riepilogo, costantemente aggiornato, delle misure di sicurezza implementate, richiamato nel Registro dei

	Trattamenti della Società.
Normativa	Si intende il Regolamento UE 2016/679, nonchè 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 con adeguata conoscenza della Normativa e delle prassi in materia di Protezione dei Dati. Il compito principale è di sovraintendere ai processi ed agli adempimenti in materia di Privacy, in collaborazione con il Titolare o 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	È il Registro tenuto obbligatoriamente, in forma scritta, ai sensi dell'art. 30 del Regolamento. La tenuta dei Registri è di norma rimessa al Referente Privacy. 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). Asco Holding, in quanto non soggetta all'obbligo di nomina, ha ritenuto di non dotarsi di un proprio DPO.
Soggetto Delegato **(o "Soggetto con funzioni di Titolare")**	Soggetto individuato nell'ambito del management della Società, 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, sono state individuate le figure che saranno illustrate nei paragrafi che seguono.

6.1 Titolare del Trattamento

Il Titolare è Asco Holding S.p.A. che opera in maniera autonoma e indipendente nel Trattamento dei Dati personali.

Nell'ambito del rapporto infragruppo, è stato concluso un accordo di "Contitolarità" con la controllata Ascopiave S.p.A., in forza del quale, le funzioni di Titolare, relativamente ai Dati personali trattati per la prestazione dei servizi generali da parte di Ascopiave, sono svolte congiuntamente dalle due Società.

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:
  - informative, consensi e gestione dei riscontri all'Interessato;
  - Registro dei Trattamenti;
  - misure di sicurezza e gestione di eventuali Data Breach;
  - Data Protection Impact Assessment (DPIA);
  - 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 del Trattamento;
11. fornisce idonee istruzioni sul Trattamento ai Responsabili del Trattamento designati;
12. designa, se del caso, 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.

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 ed è nominato formalmente dal Titolare.

Asco Holding, alla luce dell'esiguità dei Dati personali trattati, non è soggetta all'obbligo di nomina del DPO, ma ha facoltà di provvedervi.

6.4 Referente Privacy

Come riportato al paragrafo 1 del presente Manuale, Asco Holding, nell'ambito del contratto di servizio, si avvale della funzione Referente Privacy di Ascopiave.

Il Referente Privacy ha il compito di sovraintendere ai processi ed agli adempimenti in materia di Privacy, in collaborazione con il DPO di Ascopiave 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 di Asco Holding e, in tal senso, supporta il Titolare (e/o l'eventuale Soggetto Delegato).

Compiti principali del Referente Privacy sono:

1. coordinare le esigenze informatiche (ambienti e accessi) del personale di Asco Holding;
2. fornire consulenza ed assistenza operativa agli addetti di Asco Holding 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 delle banche Dati affidate alla sua gestione, sia informatizzate che cartacee, nonché svolgere le verifiche e le attività previste dalle Procedure vigenti rispetto agli accessi agli applicativi propri del personale di Asco Holding e ad eventuali soggetti esterni, cui avessero ad essere assegnati;
5. gestire, con la supervisione della Funzione Privacy, 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 di Asco Holding che, nel normale esercizio delle proprie mansioni, sono chiamati a trattare i Dati.
Ad ognuno, il Titolare (o il Responsabile) del Trattamento 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;
2. lasciare incustoditi, nemmeno per brevi periodi:
   a) documenti contenenti i Dati;
   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, cassetti e/o armadi;
- effettuare il log off e spegnere il proprio pc;

10. informare tempestivamente, o segnalare al Focal Point di riferimento, ove nominato, o alla Funzione Privacy:
    - 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, 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.

In virtù del Contratto di Servizio vigente, citato al paragrafo 1, Asco Holding potrebbe altresì avvalersi dei Focal Point nominati da Ascopiave.

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, oltre agli obblighi propri di ogni Autorizzato 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

Come riportato al paragrafo 1 del presente Manuale, Asco Holding, nell'ambito del contratto di servizio, si avvale della Funzione Privacy propria di Ascopiave.

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 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

Come riportato al paragrafo 1 del presente Manuale, Asco Holding, nell'ambito del contratto di servizio, si avvale degli Amministratori di Sistema nominati, mediante specifica lettera di incarico, da Ascopiave.

Gli Amministratori di Sistema possono essere interni, cioè individuati tra i dipendenti di Asco Holding (e/o di Ascopiave), o esterni, cioè individuati tra le persone fisiche, professionisti e/o dipendenti di ditte fornitrici, alle quali sia stata affidata la gestione dei sistemi informativi.

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.

Gli Amministratori di Sistema sono dotati di credenziali amministrative dei sistemi informatici e possono accedere in modo continuativo a tali sistemi (attraverso i quali possono essere effettuati Trattamenti di Dati personali), senza necessità di richiedere, di volta in volta, la relativa autorizzazione.

Come precisato nelle definizioni, ai fini della presente Policy, agli Amministratori di Sistema sono assimilati gli Amministratori di data base. Dunque, rispetto a questi ultimi e con riguardo ai data base nella disponibilità di ognuno, trova applicazione analogica quanto previsto al presente paragrafo ed in genere nella presente Policy, ancorché in riferimento agli Amministratori di Sistema.

6.10 Amministratore dei sistemi di videosorveglianza con funzioni di responsabilità e

Amministratore dei sistemi di videosorveglianza

L'Amministratore dei sistemi di videosorveglianza con funzioni di responsabilità e l'Amministratore dei sistemi di videosorveglianza sono nominati dal Titolare, nei casi in cui la/e sede/i aziendale/i sia/no munita/e di apparati di videosorveglianza, mediante specifiche lettere di incarico, nelle quali sono dettagliati i compiti e le responsabilità assegnati a ciascuna funzione.

Le nomine, al pari dell'adozione di un Regolamento aziendale sulla videosorveglianza, sono obbligatarie nel caso in cui la Società sia proprietaria o conduttrice di immobili e/o di aree soggette a videosorveglianza.

Copia di ogni atto di nomina è inoltrata al Referente Privacy

Le responsabilità dell'Amministratore dei sistemi di videosorveglianza con funzioni di responsabilità e 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 adottato da Ascopiave, salvo ed impregiudicato quanto ulteriormente previsto dall'Autorità di controllo.

In particolare, l'Amministratore dei sistemi di videosorveglianza con funzioni di responsabilità, con la collaborazione ed il supporto degli Amministratori dei sistemi di videosorveglianza, deve assicurarsi che l'utilizzo degli impianti di videosorveglianza avvenga nel rispetto dei principi applicabili al Trattamento dei Dati ed esclusivamente per finalità determinate, esplicite e legittime.

Il Regolamento aziendale sulla videosorveglianza dovrà precisare, nel dettaglio, le mansioni affidate all'Amministratore dei sistemi di videosorveglianza con funzioni di responsabilità e agli Amministratori dei sistemi di videosorveglianza.

7. Adempimenti generali per il Trattamento dei Dati personali

7.1 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 i dati di contatto del Titolare;
- i dati del contatto del DPO, se nominato;
- 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.

7.2 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 ovvero 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", il consenso esplicito dell'Interessato non è necessario, fermo l'obbligo di informativa ai sensi del punto 7.1 ed il rispetto di quanto previsto ai punti che seguono.

7.3 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 e salvi peculiari obblighi di conservazione previsti dalla normativa applicabile pro tempore vigente, 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.

7.4 Riservatezza del Trattamento dei Dati e loro classificazione

Ai soggetti che trattano i Dati è fatto assoluto divieto di utilizzare gli stessi per i propri scopi privati e/o renderli accessibili a qualsiasi soggetto non autorizzato, quindi di utilizzarli e/o divulgarli 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 di Asco Holding 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.

7.5 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 Titolale, 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.).

A seconda della categoria di Dati e dei conseguenti rischi associati al Trattamento, devono adottarsi 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).

7.6 Dati personali relativi a condanne penali e reati

Ai sensi dell'art. 10 del GDPR, il Trattamento di Dati relativi alle condanne penali ed ai reati 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.

7.7 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 (ove nominati), 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 del Trattamento.
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 Contitolare e (nell'eventualità) del Responsabile del Trattamento;
- le strutture aziendali 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 Focal Point (se nominati), o i singoli Autorizzati, 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 del Trattamento in capo ad Asco Holding e/o l'avvenuta nomina di nuovi Responsabili del Trattamento da parte della Società e/o l'intervenuta modifica di Trattamenti esistenti.
In dette circostanze, i Focal Point o gli Autorizzati, trasmettono altresì al Referente Privacy la documentazione a supporto (es. copia degli atti da cui derivano le esigenze anzidette, testi delle Informative impiegate, atti di nomina a Responsabile del Trattamento, ecc.).

7.8 Formazione

Il Titolare assicura a tutti gli Autorizzati al Trattamento ed in genere al personale dipendente, una formazione adeguata rispetto alla Normativa ed alle 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 e curato dalla Funzione Privacy.

7.9 Trasferimento di Dati personali

Premettendo che, nel contesto operativo di Asco Holding, trattasi di 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.

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

Asco Holding 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 e nel contesto di Asco Holding, il referente dell'Autorità è l'intera Funzione Privacy.

I Focal Point ed in genere tutti gli Autorizzati e qualunque dipendente devono cooperare con 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 della Funzione Privacy, è fatto obbligo ad ogni dipendente, collaboratore e/o consulente di Asco Holding 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, o referente contrattuale.

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 (se nominato) oppure alla Funzione Privacy, fornendo ogni informazione utile alla successiva gestione.

7.11 Monitoraggio della conformità

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

8. Adempimenti particolari disciplinati dal GDPR

8.1 Diritti degli Interessati e gestione delle richieste di esercizio degli stessi

Il Titolare garantisce agli Interessati l'esercizio dei diritti riconosciuti a questi ultimi, in conformità con quanto stabilito e richiesto dalla Normativa. In particolare, ogni Interessato, oltre alla facoltà di presentare reclamo all'Autorità di vigilanza, 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 personali 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 sia stato revocato il consenso su cui si basa il Trattamento, 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.

In generale, rispetto agli adempimenti conseguenti all'esercizio dei diritti degli Interessati:

- il Titolare del Trattamento adotta le misure tecniche e organizzative necessarie a favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli Interessati (che dovranno avere la forma scritta, anche elettronica);
- il termine per la risposta all'Interessato è, normalmente di 30 giorni, estendibile fino a 90 giorni in casi di particolare complessità;

- all'Interessato deve essere fornito un riscontro entro 30 giorni dalla richiesta anche in caso di diniego;
- il riscontro all'Interessato, di regola, deve avvenire in forma scritta; può essere dato oralmente solo su espressa richiesta dell'Interessato (art. 12, co.1 e art. 15, co. 3 del Regolamento);
- la risposta fornita all'Interessato deve essere intelligibile, concisa, trasparente, facilmente accessibile e utilizzare un linguaggio semplice e chiaro;
- ove coinvolto, il Responsabile del Trattamento è tenuto a collaborare con il Titolare ai fini dei riscontri all'esercizio dei diritti degli Interessati (art. 28, co. 3, lettera e) del Regolamento).

Ogni Interessato può inviare le richieste volte all'esercizio di uno o più dei diritti di cui sopra, per iscritto:

- a mezzo e-mail, all'indirizzo di posta elettronica privacy@ascopiave.it, o altro eventualmente previsto;
- a mezzo posta, c/o la sede di Asco Holding S.p.A., all'attenzione del Referente Privacy.

Il Referente Privacy è la funzione normalmente preposta alla gestione di tali richieste.

Qualora le richieste avessero a pervenire a recapiti diversi rispetto a quelli sopra indicati, le stesse dovranno essere inoltrate tempestivamente, dal personale ricevente, al Referente Privacy (alla e-mail privacy@ascopiave.it).

Il Referente Privacy, verificata l'identità del richiedente, con la collaborazione delle funzioni aziendali interessate, adotta le condotte e svolge le attività necessarie ad accertare la sussistenza dei presupposti per l'esercizio del diritto invocato e quindi a dare tempestivo riscontro all'Interessato.

Il Referente Privacy cura altresì la tenuta di un registro di sintesi delle richieste pervenute ad Asco Holding (di seguito "Registro richieste"), motivate dalla volontà di esercitare uno o più dei diritti riconosciuti all'Interessato.

Alla ricezione di un'istanza volta all'esercizio di un diritto dell'Interessato, il Referente Privacy, con la collaborazione della funzione aziendale incaricata e con l'assistenza, ove necessario, della Funzione Privacy, provvede all'espletamento delle seguenti attività di base:

A. accertamento in merito all'effettiva esistenza del Trattamento, cui la richiesta fa riferimento;
B. eventuale identificazione dei Focal Point e/o della funzione aziendale interessati;
C. individuazione dei Dati afferenti l'Interessato, a seguito del riscontro ottenuto con l'individuazione di cui alla lett. B;
D. verifica dell'eventuale presenza dei Dati dell'Interessato all'interno di sistemi e/o archivi di terze parti e conseguente presa di contatto con queste ultime, ove necessario, per comunicare la ricezione della richiesta di accesso da parte dell'Interessato;
E. trasmissione del riscontro positivo, o motivatamente negativo, preferibilmente mediante formato elettronico (e-mail), ovvero a mezzo lettera raccomandata, pec, o posta prioritaria,

esclusivamente ai recapiti indicati dall'Interessato. La comunicazione deve contenere le sole informazioni richieste e non vanno trasmessi Dati di soggetti terzi;

F. nel caso, impartire alle funzioni aziendali competenti le istruzioni necessarie in merito agli adempimenti da porre in essere in ragione ed ai sensi del riscontro fornito;

All'esito delle attività anzidette, il Referente Privacy archivia, di norma in formato elettronico, la documentazione conseguente alla ricezione (e gestione) della richiesta, provvedendo altresì alla compilazione del Registro richieste.

8.2 Data Breach e flussi comunicativi all'Autorità

Gli Autorizzati al Trattamento, 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 (ove nominato) o al Responsabile aziendale di riferimento (ma, nel caso, anche direttamente 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 o il Responsabile aziendale 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, 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, 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.

8.3 Data Protection Impact Assessment e misure di sicurezza

Il Titolare, nei casi e secondo le modalità previste dalla Normativa, e conformemente al principio di Accountability, assicura che, prima di procedere ad un nuovo Trattamento (e/o prima di attuare modifiche significative su un Trattamento, in ipotesi, già in essere), che si caratterizzi per l'elevato rischio rispetto alla possibile compromissione delle libertà e dei diritti degli Interessati, venga effettuata una valutazione d'impatto sulla protezione dei Dati (Data Protection Impact Assessment). La DPIA viene svolta attraverso un apposito software adottato dal Titolare e messo a disposizione dal Garante per la Protezione dei Dati personali francese.

Ogni Autorizzato, o ciascun Focal Point (ove nominato) è tenuto a monitorare i Trattamenti in essere e/o da avviare nella propria area di competenza, quindi a segnalare, alla Funzione Privacy, ogni situazione in cui possa rendersi necessaria l'espletamento di una valutazione di impatto.

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, sentita la Funzione Privacy, prima di procedere al relativo Trattamento, consulta l'Autorità di controllo.

8.4 Privacy by Design

Conformemente a quanto stabilito dal Regolamento all'art. 25, la Privacy by Design ("PbD") sintetizza una serie di principi atti a sottolineare la centralità che gli aspetti Privacy (quindi la tutela dei Dati personali) dovrebbero rivestire in qualsiasi ambito, scelta o azione intrapresa da parte dei Titolari o Contitolari, o Responsabili al Trattamento (o soggetti che intendono assumere tali status rispetto ad un potenziale nuovo Trattamento), ai sensi del GDPR.

La PbD prevede, in particolare, che la protezione dei Dati personali degli Interessati sia presa in considerazione sin dal momento della determinazione delle modalità e dei mezzi con cui sarà svolto il Trattamento e, in seguito, costantemente monitorata. La PbD intende perciò garantire l'osservanza dei principi del GDPR durante l'intero ciclo di vita del sistema e/o della tecnologia utilizzata, dalle prime fasi di progettazione fino al termine della sua "vita tecnica".

Gli elementi fondamentali della PbD sono enunciati in sette punti principali, già riconosciuti e adottati dal Gruppo di Lavoro dei Garanti Privacy Europei:

1. adozione di un approccio proattivo, non reattivo;
2. definizione della Privacy come parametro predefinito;
3. necessità di tenere in considerazione i rischi Privacy fin dalle fasi di progettazione di un nuovo Trattamento e/o di un sistema che tratti Dati personali;
4. massima funzionalità;
5. applicazione della sicurezza sull'intero ciclo di vita / esistenza del Trattamento;
6. visibilità e trasparenza;

7. rispetto dei diritti dell'Interessato per l'intero ciclo di vita del Trattamento dei Dati personali del medesimo.

Trattandosi di una tematica legata sia al principio di "accountability" che al principio di "by default" [2], la PbD trova applicazione ogni qualvolta sopravvengano modifiche allo *status quo*, indipendentemente dalle aree di business o dalle funzioni coinvolte.

A titolo di esempio, si riporta un elenco, non esaustivo, degli scenari di cambiamento che, potenzialmente, potrebbero necessitare di un vaglio in termini di PbD:

- nuovo processo aziendale, o modifica / integrazione sostanziale di un processo aziendale già in essere;
- nuovo contratto stipulato con fornitori e/o partner, o modifica a contratti attualmente in essere;
- qualsiasi altra modifica rilevante, da valutarsi in un'ottica di analisi rischi (quindi, ad esempio, cambio sede o apertura nuovi uffici, cambi rilevanti organizzativi, etc.).

Qualora da detti eventi possa derivare a) un impatto, più o meno significativo, sui Trattamenti in essere, ovvero b) l'esigenza di avviare Trattamenti nuovi, il Focal Point di riferimento, o altro soggetto titolato informa la Funzione Privacy.

Eseguite le opportune valutazioni, La Funzione Privacy comunicherà le eventuali azioni correttive da porre in essere affinché le modifiche allo *status quo* avvengano nel rispetto delle libertà e dei diritti degli Interessati.

8.5 Data Retention

L'art. 5 del Regolamento stabilisce che i Dati personali debbano essere conservati per un periodo non superiore a quello necessario agli scopi per il quali sono stati raccolti e trattati.

Le tempistiche di conservazione dei Dati, quando non sono stabilite dall'Autorità di controllo, devono essere determinate dal Titolare.

Rispetto ai principali Trattamenti connessi all'ordinaria attività di Asco Holding, il riferimento base è alla tabella "Termini di Retention", allegato alla presente Policy. I termini ivi indicati tengono conto, anzitutto, dell'ordinario limite di prescrizione di cui all'art. 2946 cc, con riguardo a quelle tipologie di Trattamento rispetto alle quali potrebbero emergere (appunto entro il termine di prescrizione) contestazioni e/o contenziosi, nonché dei termini previsti per l'espletamento di verifiche da parte di Enti e/o Autorità pubbliche, ovvero dei termini di conservazione della documentazione (es. ai fini fiscali). Eventuali deroghe ai limiti indicati in tabella possono essere previste, in via preventiva, per il singolo Trattamento, con esplicitazione delle relative motivazioni.

[2] Il principio di By Default impone al Titolare del Trattamento di porre in essere meccanismi volti a garantire, quale impostazione predefinita, che oggetto del Trattamento siano unicamente quei Dati strettamente necessari al perseguimento delle specifiche finalità per cui sono stati raccolti.

Nel Registro dei Trattamenti si darà indicazione del termine di retention mediante esplicito richiamo ad una delle categorie di Trattamento incluse nella tabella di cui all'allegato "Termini di Retention". Per i Trattamenti non rientranti in nessuna delle categorie ivi presenti, il termine di retention sarà indicato direttamente nel Registro.

Alla fine del periodo di retention, i Dati, ove possano escludersi rischi per i diritti degli Interessati e/o per i diritti del Titolare, sono cancellati e/o distrutti. In tutti i casi in cui, al termine del periodo di retention, non sia possibile provvedere con immediatezza alla Cancellazione o Distruzione definitiva dei Dati, si potrà provvedere, alternativamente o cumulativamente (a seconda della casistica concreta):

1. a rendere i Dati inaccessibili, quindi non più utilizzabili/consultabili per gli utenti muniti delle ordinarie credenziali di accesso (proprie degli Autorizzati al Trattamento);
2. a crittografare i Dati, rendendoli non più comprensibili ai medesimi utenti;
3. ad adottare altre similari condotte volte a rendere inutilizzabili ed inconsultabili i Dati, al pari di quanto accadrebbe a seguito della loro Cancellazione o Distruzione definitiva, o tali da rendere anonimo e non più identificabile il relativo Interessato.

Al raggiungimento dei termini di retention, sarà cura del Referente Privacy fornire le necessarie indicazioni agli Amministratori di Sistema e nel caso alle altre funzioni aziendali coinvolte, affinché provvedano di conseguenza, in conformità al presente Manuale.

I Focal Point (ove nominati), o gli Autorizzati hanno l'onere di segnalare al Referente Privacy quei Trattamenti rispetto ai quali gli stessi abbiano contezza della prossima scadenza del termine di retention.