Aristoncavi SpA

Policy: Personal Data Protection

Sommario

1. Scopo e ambito di applicazione

La Personal Data Protection Policy disciplina a livello generale la gestione dei dati personali, definisce ruoli e responsabilità inerenti a tale gestione e disciplina alcuni processi specifici. La policy è integrata dall'impianto normativo interno di Aristoncavi, di seguito la "Società".

La presente politica, i suoi allegati, le altre politiche, le linee guida, le procedure e le istruzioni, formalizzate e verbali, costituiscono l'impianto normativo interno e rappresentano le istruzioni al trattamento dei dati personali ai sensi dell'art. 29 del Regolamento (UE) 2016/679 affinché chiunque agisca sotto l'autorità del Controller sia adeguatamente istruito nell'esecuzione dei trattamenti dei dati personali.

2. Distribuzione

A tutti i dipendenti e collaboratori.

3. Terminologia, abbreviazioni, definizioni

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
Titolare: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

4. Riferimenti

- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati o GDPR).
- Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)
- Decreto Legislativo n. 196 del 30 giugno 2003 "Codice in materia di protezione dei dati personali" e successivi provvedimenti emanati dall'Autorità Garante per la protezione dei dati personali e normative successive o particolari.

5. Nota importante

La presente policy riprende alcune terminologie, definizioni e concetti della normativa applicabile allo scopo informativo e divulgativo in merito alla stessa.
Si noti che

- I concetti sono volutamente sintetizzati, quindi la lettura della presente policy non esime dalla conoscenza di quanto indicato in modo più esteso dalla normativa.
- In caso di elementi di contraddizione tra la presente policy e la normativa applicabile vale quanto definito in quest'ultima.
- Fatto salvo quanto indicato nel punto precedente, le disposizioni della presente policy devono essere applicate.

6. La normativa applicabile

a. Premessa

L'evoluzione tecnologica dei sistemi per l'informazione sta portando ad una più veloce e più profonda condivisione delle informazioni e dei dati. Tra questi vi sono i dati personali, relativi alle persone fisiche. Tali dati non sono limitati ai dati identificativi, ma sono costituiti da qualsiasi dato che ci riguarda. Ad esempio attraverso anche la semplice navigazione in Internet, senza nemmeno accorgerci, divulghiamo i nostri dati personali che possono essere utilizzati per studiare le nostre abitudini di consumo. L'evoluzione della normativa in materia di protezione dei dati mira a definire delle regole per limitare questa invasività nella vita personale, pur riconoscendo i diritti delle società a svolgere attività di marketing.

L'Europa si è fatta promotrice di una serie di iniziative a livello normativo. Dalla Convenzione di Strasburgo (n. 108 del 28/01/81), ratificata con la L. 98 del 21/02/1989, all'accordo di Schengen e successivamente alla Direttiva 95/46/CE e alla Direttiva 2002/58/CE, ispiratrici dell'attuale Codice Privacy, D. Lgs 196/2003.

Nel 2016 è stato pubblicato il regolamento generale sulla protezione dei dati, Regolamento UE 2016/679, (di seguito "Regolamento", o "GDPR" – General Data Protection Regulation –), primo tassello di una serie di riforme attraverso le quali la Commissione europea intende rafforzare e rendere più omogenea la protezione dei dati personali di cittadini dell'Unione Europea e dei residenti nell'Unione Europea, sia all'interno che all'esterno dei confini dell'Unione europea (UE).
Il testo, pubblicato su Gazzetta Ufficiale Europea il 4 maggio 2016 ed entrato in vigore il 25 maggio dello stesso anno, ha efficacia dal 25 maggio 2018. Il GDPR abroga la direttiva sulla protezione dei dati (Direttiva 95/46/EC).

b. I principi

Il Regolamento sancisce i seguenti principi applicabili ai dati personali (art. 5).
I dati personali sono:

a. trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
b. raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; […] («limitazione della finalità»);
c. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
d. esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
e. conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; […] («limitazione della conservazione»);
f. trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

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

c. Le basi giuridiche del trattamento

i. Liceità del trattamento

Sulla base di quanto definito dal Regolamento nell'art. 6, il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a. l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b. il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c. il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
d. il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e. il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
f. il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

ii. Trattamento di categorie particolari di dati personali

È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona; salvo che non ricorra uno dei seguenti casi:

a. l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto […]
b. il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;
c. il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
d. il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;
e. il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
f. il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
g. il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri […];
h. il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali […];

i. il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica […];
j. il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici […].

iii. Trattamento dei dati personali relativi a condanne penali e reati

Secondo quanto definito dall'art. 10 il trattamento dei dati personali relativi alle condanne penali e ai reati […] deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica

d. Principi di privacy by design e privacy by default

Nell'ambito dell'adozione di misure tecniche ed organizzative adeguate al fine di tutelare i dati da trattamenti illeciti, il Regolamento introduce all'art 25 i principi di **privacy by design** e **privacy by default**, fornendo un approccio nuovo che impone alle aziende l'obbligo di prevedere sin da subito, all'avvio di ogni progetto, strumenti a tutela dei dati personali.

i. Protezione fin dalla progettazione

Il concetto di privacy by design è basato sulla valutazione del rischio. Tale valutazione deve essere effettuata al momento della progettazione dei sistemi e dei servizi offerti, quindi prima che il trattamento abbia luogo. Un approccio basato sul rischio comporta la necessità di tenere conto dello stato della tecnologia, pertanto il trattamento dovrà essere adattato ai cambiamenti nel corso del tempo.
Il controller mette in atto le misure tecniche e organizzative adeguate ad attuare i principi di protezione dei dati e ad integrare le garanzie necessarie, nel rispetto anche del cd. principio di accountability che permea il GDPR.

ii. Protezione per impostazione predefinita

Il concetto di privacy by default è basato sull'assunto che qualsivoglia progetto o prodotto debba garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento, con riferimento alla qualità dei dati raccolti, alla portata del trattamento, al periodo di conservazione e all'accessibilità.
Privacy by default quindi come non eccessività dei dati raccolti, ma anche come garanzia di non accessibilità ad un numero indefinito di persone fisiche ai dati degli interessati.

e. Autorità

Il Regolamento, oltre a confermare la definizione di un'autorità di controllo per ogni Stato Membro, ne disciplina la competenza, i compiti ed i poteri e disciplina inoltre i protocolli di comunicazione tra autorità a livello europeo ed i relativi meccanismi di coordinamento.

In Italia l'autorità di controllo prende nome di **Garante per la protezione dei dati personali**.

Il Regolamento istituisce inoltre a livello europeo il **Comitato di controllo per la protezione dei dati**, composto dal vertice delle autorità di controllo locali al quale assegna maggiori poteri rispetto a quelli posseduti dal gruppo di lavoro dei garanti ex art. 29 della Direttiva 95/46/CE, detto **WP29**.

7. I ruoli e le responsabilità

a. Soggetti previsti dalla normativa

i. Controller

Nella terminologia italiana è indicato come **Titolare** ed è definito come la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

ii. Processor

Nella terminologia italiana è indicato come **Responsabile del trattamento** ed è definito come la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.
Il Titolare ricorre ai Responsabili del trattamento nei rapporti di esternalizzazione nei quali siano previsti, da parte della terza parte, trattamenti di dati personali per conto del Titolare.
La nomina di responsabile deve essere un atto formale espletato attraverso l'apposito modulo di nomina, dove sono specificati altresì i compiti e le responsabilità del Processor.

b. Altri soggetti preposti ai trattamenti

i. Referente Privacy

Il Referente Privacy collabora con il Controller ed il Processor nel garantire il rispetto della presente Policy, del Regolamento e della normativa vigente:

- monitorando le principali modifiche nella normativa vigente e mantenendosi aggiornato;
- fornendo consulenza interna e istruendo, laddove necessario, il Personale Autorizzato e tutti gli interessati sul tema della privacy;
- segnalando eventuali violazioni di dati trattati, di qualsiasi natura e tipologia;
- garantendo, anche su segnalazione dei responsabili delle aree, i diritti spettanti agli interessati del trattamento (accesso, informazione, rettifica, oblio e limitazione).

Il Referente Privacy viene selezionato autonomamente dalla Società al suo interno e possibilmente in base a ruolo, esperienza e competenze tali da renderlo adeguato ai compiti sopraelencati.

ii. Personale Autorizzato

Si definisce Personale Autorizzato qualsiasi lavoratore della Società, con qualsiasi forma contrattuale, che nell'ambito delle proprie mansioni accede a dati personali di persone fisiche, sotto l'autorità del Titolare o del Responsabile.
Il Personale Autorizzato, nell'ambito del trattamento di dati personali e di qualsiasi altra informazione aziendale, si deve attenere, ai sensi dell'art. 29 del Regolamento, alle istruzioni scritte presenti nella presente policy e nel resto dell'impianto normativo interno applicabile. In particolare ha i seguenti compiti:

- Conoscere il contenuto della presente politica e dell'impianto normativo interno applicabile alla sua mansione.
- Osservare e attuare le prescrizioni normative, di questa politica e dell'impianto normativo interno applicabile alla sua mansione.
- Collaborare per l'applicazione dei principi del Regolamento e per il miglioramento delle misure di protezione

- Rispettare le disposizioni in ordine alla gestione dei trattamenti dei dati nell'ambito delle proprie competenze.
- Informare tempestivamente il proprio responsabile o il Referente Privacy in caso di identificazione o di sospetto di una violazione (data breach).
- Informare tempestivamente il proprio responsabile o il Referente Privacy nel caso un interessato eserciti i propri diritti in base al capo III del Regolamento.
- Informare tempestivamente il Referente Privacy nel caso ravvisi eventuali violazioni della normativa, di questa policy o dell'impianto normativo interno.

iii. Amministratore di Sistema

L'Amministratore di Sistema è qualsiasi figura che svolge un ruolo nella gestione dei sistemi informatici determinante dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori dei server, gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.
La base normativa di riferimento è costituita dal Provv. Garante doc. web n. 1577499, del 27 novembre 2008.
Le istruzioni scritte ai sensi dell'art. 29 del Regolamento, oltre a quanto previsto nella presente policy e nell'impianto normativo interno, sono dettagliate anche all'interno della nomina formale appositamente predisposta.

8. Politica di Sicurezza delle informazioni

a. Politica per i dispositivi

Tutti gli Utenti della Società che, per specifiche esigenze lavorative utilizzino ai fini lavorativi dispositivi quali ad esempio desktop, PC portatili, telefonini cellulari e altre apparecchiature portatili, devono prestare la massima cura affinché le informazioni contenute in questi strumenti non vengano compromesse.

Gli assegnatari di tali dispositivi non possono prestarli, noleggiarli o comunque darli in uso a terzi, interni o esterni, non assegnatari.

Non possono essere utilizzati desktop o PC portatili personali per l'attività lavorativa. Eventuali eccezioni devono essere autorizzate dalla Direzione previa consultazione con la funzione IT.

Tutti i dispositivi informatici e le dotazioni (ad esempio PC, smartphone, scrivania, cassettiera, armadi, ecc.) sono assegnati al lavoratore solo ed unicamente per lo svolgimento delle attività lavorative, precisando che tutti i dati e le informazioni contenute sui supporti di vario genere sono di proprietà della società.

La Società si riserva il diritto di svolgere attività di audit o accedere per ragioni di servizio a tutte le informazioni presenti sugli strumenti utilizzati ai fini lavorativi. Ove possibile, il lavoratore sarà avvisato prima di accedere alle informazioni, altrimenti in un momento successivo a tale accesso.

Ai fini della gestione della sicurezza come l'analisi degli incidenti, l'individuazione di tentativi di intrusione da parte di terzi e la protezione delle informazioni, le attività svolte dagli utenti come l'utilizzo delle risorse informatiche, le attività sui sistemi operativi, la navigazione Internet potrebbero essere tracciate.

b. Gestione delle credenziali

- La password iniziale, valida esclusivamente per l'effettuazione della prima connessione, deve essere comunicata in modo riservato all'Utente destinatario e deve essere immediatamente sostituita dall'Utente. L'Utente non deve effettuare alcuna operazione se prima non ha provveduto a sostituire la password iniziale.

- La lunghezza minima della password deve essere almeno di otto caratteri. Nel caso in cui il sistema non imponga una password di lunghezza minima l'Utente dovrà comunque attenersi alla disposizione.
- La password scelta dall'Utente non deve essere banale o facilmente individuabile (es. password identica alla User ID, password contenente riferimenti agevolmente riconducibili agli incaricati, ecc.). Laddove possibile deve contenere caratteri alfabetici, maiuscoli e minuscoli, caratteri numerici e caratteri speciali.
- Le password hanno una durata massima di 90 giorni trascorsi i quali le password devono essere sostituite.
- La password deve essere mantenuta segreta ed è vietata qualsiasi forma di comunicazione della stessa.

c. Gestione dei backup

La Società definisce le politiche di backup, la conservazione dei supporti di registrazione e gli eventuali ripristini devono essere gestiti consentendo oltre al corretto salvataggio anche il ripristino dei dati entro le tempistiche previste. Tali politiche devono prevedere al minimo:

- Devono essere previsti backup almeno settimanali.
- Deve essere prevista la conservazione dei supporti dei backup in un luogo diverso rispetto al luogo in cui sono presenti i server soggetti a backup. La distanza tra i due luoghi deve garantire la sicurezza fisica della conservazione dei dati in caso di eventi di rischio.
- Devono essere garantiti dei tempi di ripristino dei dati coerenti con le necessità di business della Società.

Tutti gli Utenti devono essere informati delle politiche di backup dei dispositivi utilizzati.

d. Gestione degli accessi

L'accesso ai Sistemi Informativi deve essere controllato attraverso un processo formale di creazione, modifica e cancellazione degli account assegnati agli Utenti, che preveda il coinvolgimento del business per definire privilegi consoni alla mansione svolta.

Tutti gli Utenti devono possedere identificativi unici personali (user ID) associati ad una password per l'autenticazione. Le user ID non devono fornire alcuna indicazione dei livelli di autorizzazione concessi all'Utente specifico.

L'assegnazione e l'utilizzo di utenze privilegiate deve essere limitato e controllato.

Deve essere definita un'attività periodica, almeno annuale, di controllo delle utenze al fine di verificare che le stesse siano assegnate ad Utenti che hanno le qualità per accedere ai sistemi e che i privilegi ad essi assegnati siano coerenti con la loro mansione.

e. Gestione degli archivi

Ogni Persona Autorizzata deve gestire le informazioni riducendo al minimo il supporto cartaceo che deve essere mantenuto ordinato, eventualmente attraverso appositi raccoglitori, e che deve essere custodito con regole di sicurezza coerenti con la criticità del contenuto stesso. Nel caso di informazioni critiche, di dati che appartengono alle categorie particolari, o più genericamente di dati che possono avere un impatto sulla libertà e dignità degli interessati, i supporti cartacei devono essere conservati in un luogo ad accesso limitato, per esempio chiuso a chiave. Deve essere definito un processo di gestione delle autorizzazioni.

f. Clear Desk

Per ridurre al minimo i rischi di accesso non autorizzato, perdita e modifica delle informazioni, devono essere adottate una serie di norme comportamentali di seguito descritte.

L' Utente deve:

- Accertarsi che le impostazioni dei dispositivi consentono lo sblocco solo attraverso l'inserimento di User ID e password.
- Impostare manualmente il blocco dei dispositivi nel momento in cui lascia temporaneamente incustodita la postazione di lavoro.
- Accertarsi che le impostazioni dei dispositivi consentono il blocco automatico degli stessi dopo un periodo limitato di tempo durante il quale non vengono utilizzati (ad esempio 2/3 minuti).
- Quando si visualizzano informazioni critiche su uno schermo, accertarsi che le informazioni non siano viste da soggetti terzi non autorizzati.
- Le informazioni di business riservate o critiche, sia su carta, sia su supporti di memorizzazione digitale, quando non utilizzate devono essere riposte in un luogo protetto e ad accesso limitato;
- Non devono essere lasciati incustoditi documenti contenenti dati durante e dopo l'orario di lavoro;
- Limitare allo stretto necessario l'effettuazione di copie dei suddetti documenti. La riproduzione di documenti contenenti dati sensibili su supporti non informatici (ad esempio, fotocopie) deve essere sottoposta alla medesima disciplina dei documenti originali;
- Le stampe contenenti informazioni riservate devono essere rimosse immediatamente dalle stampanti. Laddove tecnicamente possibile utilizzare forme di stampa protetta.
- La distruzione dei supporti cartacei deve comunque garantire la sicurezza delle informazioni, ad esempio strumenti di distruzione dei documenti.

g. Configurazioni

È vietata l'installazione autonoma di qualsiasi software o di qualsiasi aggiornamento dei software esistenti sulle dotazioni assegnate. La necessità di tali installazioni deve essere segnalata alla Direzione.

È altresì vietata qualsiasi modifica alla configurazione, hardware e software, degli strumenti aziendali assegnati

L'introduzione in azienda di un qualsiasi tipo di sistema informatico o di servizio eseguito per mezzi informatici deve essere preventivamente valutata dalla Direzione.

L'accesso a Internet può essere effettuato solo attraverso strumenti aziendali la cui connessione è protetta da appositi dispositivi di sicurezza, quali Firewall, Proxy Server, Antivirus.

È vietato utilizzare connessioni alternative a quelle aziendali per accedere ad Internet dalla propria postazione di lavoro (ad esempio connessione wifi libere o personali). Per aumentare il livello di protezione della propria rete, la Società si riserva la facoltà di adottare un sistema di blocco o filtro automatico per vietare l'accesso a siti non pertinenti all'attività lavorativa.

L'accesso a qualsiasi tipo di sistema informatico aziendale da parte di fornitori o terze parti deve essere autorizzato dalla Direzione.

h. Email

La casella di posta elettronica assegnata all'Utente è uno strumento di lavoro e deve essere utilizzata esclusivamente per finalità connesse allo svolgimento dell'attività lavorativa.

Disposizione per l'uso dell'email aziendale:

- Sono vietate le comunicazioni di natura privata, personale, per scopi estranei allo svolgimento della prestazione lavorativa e/o di collaborazione.

- È vietato inviare, senza le necessarie autorizzazioni, materiale protetto da copyright, o vietato dalle leggi in vigore o dalle procedure aziendali nel loro complesso. Nel caso tale materiale sia ricevuto bisogna prontamente darne informazione al proprio responsabile affinché l'azienda possa prendere gli opportuni provvedimenti.

- È' vietato inviare o inoltrare, sia all'interno dell'azienda, sia ad indirizzi esterni, e-mail con messaggi non attinenti all'attività lavorativa e messaggi con "comunicazioni a catena". I messaggi sospetti (anche indicanti eventuali modalità di rimozione di virus, o con link sospetti) devono essere prontamente segnalati alla funzione IT, evitando di cliccare su link o su allegati.

- È vietata la configurazione di client di posta del PC o del Laptop aziendale per accedere alla posta da account non aziendali. Questi possono eventualmente essere acceduti in situazioni di eccezionalità al di fuori dell'orario lavorativo attraverso il browser Internet installato, fermo restando il divieto assoluto di scaricarne gli allegati.

- È vietato creare o trasmettere e-mail con contenuti discriminatori, offensivi o in qualunque modo lesivi della dignità umana.

- È vietato richiedere l'invio dall'esterno o inviare all'esterno applicativi software.

- È vietato utilizzare strumenti di scambio documenti via e-mail non autorizzati a livello aziendale (come ad esempio WeTransfer, etc.)

- Non essendo il canale delle e-mail un canale sicuro, è vietato trasmette informazioni critiche o contenenti categorie di dati particolari senza aver provveduto ad adottare strumenti di cifratura del contenuto.

- Non aprire e-mail e/o allegati con contenuti anomali o sospetti (es. mittenti non aziendali sconosciuti, oppure e-mail con oggetto non coerente con quanto inviato normalmente dal mittente, con descrizione mittente non coerente con indirizzo e-mail del mittente).

- Non inviare via posta elettronica le proprie credenziali o le password a destinatari interni o esterni.

- Non comunicare la propria password personale di posta, ad alcuno, in nessuna circostanza.

Sono impostati dei limiti massimi di dimensione delle caselle di posta; l'Utente deve provvedere all'eliminazione periodica, o quantomeno al superamento dei limiti di spazio concessi, degli allegati di grandi dimensioni o delle email inutili o provvedere periodicamente all'archiviazione locale delle email.

i. Internet

L'accesso a Internet è consentito all'Utente, esclusivamente, per finalità strettamente connesse allo svolgimento della propria attività lavorativa.

Di seguito sono elencate le regole per l'utilizzo di Internet.

- È possibile navigare solo sui siti consentiti.
- Il download e l'utilizzo di documenti provenienti da siti web o http nonché il download e l'upload di archivi e file di cui la Società deve possedere regolare licenza o deve comunque essere autorizzata da terzi.
- La registrazione a siti e a servizi di newsletter necessari all'attività deve essere autorizzata dalla Direzione.
- La partecipazione a forum professionali e bacheche elettroniche necessarie all'attività lavorativa deve essere autorizzata dalla Direzione.
- L'utilizzo del canale di internet banking deve essere consentito solo ed esclusivamente al personale esplicitamente autorizzato.

- L'utilizzo di Internet per scopi diversi da quelli esplicitati dalla Società è vietato.
- Non può essere fatto alcun utilizzo di Internet in violazione della normativa vigente.
- Non può essere fatto alcun utilizzo di Internet per fini diversi da quelli lavorativi per attività relative alla Società.
- Non può essere fatto il download e l'utilizzo di crack, patch, script o applicativi atti ad aggirare o inibire, in qualsiasi modo, protezioni hardware e software ovvero ad ottenere privilegi d'accesso a qualsiasi risorsa di rete non regolarmente attribuiti.
- Non può essere utilizzato software peer-to-peer per lo scambio di file.
- Non possono essere utilizzati instant messaging al di fuori degli strumenti aziendali il cui utilizzo è limitato alle attività lavorative.
- È vietata la navigazione in siti con contenuti pornografici, pedopornografici, osceni, discriminatori, razzisti o che ledano in qualsiasi modo la dignità individuale.
- È vietato rivelare o diffondere al pubblico informazioni confidenziali o di proprietà della Società.
- Non può essere spedito, ricevuto o promosso materiale che possa essere dannoso, molesto o intimidatorio per altre persone.
- È vietato l'uso di Internet ai fini di gaming.
- È vietato scaricare materiale in violazione del diritto d'autore.
- È vietato scaricare file audio o video non attinenti l'attività lavorativa.
- È vietato scaricare autonomamente software, anche se provvisto di regolare licenza d'uso. Nei casi sia necessario deve essere contattata la funzione IT.
- È vietato modificare o mascherare le impostazioni di rete assegnate (i.e. IP address) o aggirare o disabilitare i dispositivi preposti alla gestione della sicurezza e delle comunicazioni in rete (i.e. Firewall, Proxy, Router, ecc.)

9. Processo di Data Breach Notification

a. Premessa normativa

i. Notifica all'autorità Garante

L'articolo 33 del GDPR, in materia di notifica di violazione dei dati personali di persone fisiche, prevede che il Titolare del trattamento notifichi la violazione all'Autorità di Controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, deve essere corredata con i motivi del ritardo. A tal proposito, il Responsabile del trattamento informa il Titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.
La notifica di violazione dei dati personali di persone fisiche all'autorità di controllo deve avere i seguenti contenuti minimi:

- natura della violazione dei dati personali compresi, le categorie e il numero approssimativo di interessati in questione, le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- nome e dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- conseguenze della violazione dei dati personali;
- misure adottate per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

ii. Informazione all'interessato

L'Articolo 34 del GDPR, in materia di Comunicazione di una violazione dei dati personali all'interessato, prevede che quando la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunichi la violazione all'interessato senza ingiustificato ritardo.
La comunicazione all'interessato di una violazione dei dati personali descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le seguenti informazioni:

- nome e dati di contatto del Referente Privacy o di altro punto di contatto presso cui ottenere più informazioni;
- conseguenze della violazione dei dati personali;

- misure adottate per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

La Comunicazione della violazione dei dati personali all'interessato non è obbligatoria se è soddisfatta una delle seguenti condizioni:

- esistono misure tecniche e organizzative adeguate di protezione e applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali cifrati;
- esistono misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- la comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica.

b. Procedura

Attività	Owner	Tempi
Identificazione o sospetto dell'evento di data breach	Chiunque	n/a
Comunicazione scritta (e-mail) al proprio responsabile	Chiunque	Al sospetto dell'avvenuto evento e comunque non oltre 2h
Il responsabile avvisa la Direzione	Responsabile di funzione	Dopo una pre-analisi e comunque non oltre le 4h
La Direzione esegue l'analisi e la valutazione del rischio per i diritti e le libertà delle persone fisiche e prevede la raccolta e la verifica delle seguenti informazioni: • natura della violazione dei dati personali compresi; • categorie e numero approssimativo di interessati in questione; • categorie e numero approssimativo di registrazioni dei dati personali in questione; • probabili conseguenze della violazione dei dati personali; • misure adottate per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi. I rischi che possono determinare l'obbligo di notifica prevedono che la violazione possa causare danni fisici, materiali o immateriali alla persona fisica, quali a titolo esemplificativo e non esaustivo: • perdita del controllo dei dati personali; • limitazione dei diritti; • discriminazione; • furto o usurpazione di identità; • perdite finanziarie; • pregiudizio alla reputazione; • perdita di riservatezza dei dati personali protetti da segreto professionale, o qualsiasi altro danno economico o sociale significativo per la persona interessata.	Direzione	Entro il secondo giorno (48h)

Attività	Owner	Tempi
A seconda della valutazione che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, sono previste le seguenti attività: • Notifica al Garante: in caso di data breach, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. • Comunicazione all'Interessato: in caso di data breach con rischio elevato per i diritti e le libertà delle persone fisiche	Direzione	Entro le 72 ore dall'identificazione dell'evento
Tenuta di un registro degli eventi e redazione dei verbali	Referente Privacy	n/a
Predisposizione di un fascicolo sull'evento da esibirsi, su richiesta, al Garante	Referente Privacy	Entro 5 gg dalla notifica

10. Il processo di gestione dei Diritti dell'Interessato

a. Premessa normativa

Il Capo III del Regolamento disciplina i diritti dell'interessato, che sono declinati come segue:

- **Il diritto ad essere informato** dell'esecuzione dei trattamenti, sia nel caso in cui l'acquisizione dei dati siano presso l'interessato, sia nel caso in cui l'acquisizione dei dati sia presso una terza parte. Il diritto all'informazione dell'interessato deve includere anche la modalità chiara per l'esercizio dei propri diritti (artt. 12, 13 e 14 del Regolamento).
- **Il diritto di accesso** dell'interessato (art. 15 del Regolamento) in base al quale l'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni: a) le finalità del trattamento; b) le categorie di dati personali in questione; c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali. In questo caso deve essere informato in merito all'esistenza di garanzie adeguate; d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento; f) il diritto di proporre reclamo a un'autorità di controllo; g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine; h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione […].
- **Il diritto di rettifica** (art. 16 del Regolamento) in base al quale l'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa
- **Il diritto alla cancellazione («diritto all'oblio»)** (art. 17 del Regolamento) in base al quale l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano, se sussiste uno dei motivi seguenti: a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; b) l'interessato revoca il consenso su cui si basa il trattamento come unico fondamento giuridico c) l'interessato esercita il *diritto di opposizione*; d) i dati personali sono stati trattati illecitamente; e) i dati personali devono essere cancellati per adempiere un obbligo legale; f) i dati personali riguardano un minore di anni 16 e sono stati raccolti relativamente all'offerta di servizi della società dell'informazione. Il titolare

del trattamento, se ha reso pubblici dati personali ed è obbligato a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione, adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali. I diritti alla cancellazione non si applicano nella misura in cui il trattamento sia necessario: a) per l'esercizio del diritto alla libertà di espressione e di informazione; b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento; c) per motivi di interesse pubblico nel settore della sanità pubblica; d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici; e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

- **Il diritto alla limitazione** (art. 18 del Regolamento) in base al quale, nei casi previsti dall'articolo, come situazione transitoria o su richiesta dell'interessato, l'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento (ovvero una sospensione temporanea che può divenire definita nel caso si verifichino i presupposti per cui viene chiesta la limitazione).
- **L'obbligo, da parte del titolare, di notificare a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate**, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda (art. 19 del Regolamento).
- **L'interessato ha il diritto della portabilità** (art. 20 del Regolamento), ovvero di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora il trattamento si basi sul consenso o su un contratto ai sensi dell'articolo ed il trattamento sia effettuato con mezzi automatizzati.
- **L'interessato ha il diritto di opposizione** (art. 21 del Regolamento), ovvero si può opporre in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano nei casi in cui lo stesso si basi sull'esercizio del legittimo interesse del titolare e nel caso in cui i dati personali siano trattati per finalità di marketing, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto (l'articolo precisa ulteriori casi non ritenuti applicabili alla Società).
- **L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato**, compresa la **profilazione**, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona. Quanto sopra non si applica se il trattamento è eseguito nell'esecuzione di un contratto tra interessato e titolare, se autorizzato del diritto dell'Unione e se si basa sul consenso esplicito dell'interessato.

b. Procedura

I responsabili di funzione, verificano che i trattamenti siano eseguiti previa la necessaria informativa.

L'esercizio dei diritti da parte dell'interessato sono gestiti come segue. Il titolare deve dare risposta entro 15 giorni.

Attività	Owner	Tempi
Ricezione dell'esercizio dei diritti da parte dell'interessato	Chiunque	n/a
Comunicazione al proprio responsabile	Chiunque	All'avvenuto evento e comunque non

Attività	Owner	Tempi
		oltre 1 giorno
Il responsabile di funzione indentifica i soggetti che per poteri o informazioni possono dare un contributo determinante all'esecuzione di quanto segue.	Responsabile di funzione	Dopo una pre-analisi e comunque non oltre 2 giorni
Riscontro all'interessato	Responsabile di funzione	Entro 15 giorni dalla richiesta dell'interessato
Eventuale notifica ad altri titolari	Referente Privacy	Entro 15 giorni dalla richiesta dell'interessato
Tenuta di un registro degli eventi e redazione dei verbali	Referente Privacy	n/a