Regolamento aziendale Sotacarbo SpA

REGOLAMENTO SULLA TUTELA DELLA PRIVACY

1. Finalità

Lo scopo del presente documento è definire le procedure aziendali per adempiere ai dettami del DL.gs. n. 196 del 30.06.2003 (codice per la protezione dei dati personali - c.d. Codice della Privacy) e ss.mm.ii, del D.Lgs. 101/2018 e del Regolamento EU n 679 del 2016 (General Data Protection Regulation - c.d. GDPR), in materia di privacy e trattamento dei dati personali effettuato dalla Società.

2. Definizioni

Ai fini del presente documento si applicano le seguenti 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;
- trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- limitazione di trattamento: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- profilazione: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- pseudonimizzazione: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

- titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione Europea o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione Europea 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;
- destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione Europea o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
- terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- consenso dell'interessato: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta li proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- violazione dei dati personali: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- dati genetici: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sula fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- dati biometrici: i dati personali ottenuti da un trattamento tecnico specifico 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;
- dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- stabilimento principale: a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione Europea, salvo che le decisioni sule finalità ei mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione Europea e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale; b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione Europea

o, se li responsabile del trattamento non ha un'amministrazione centrale nell'Unione Europea, lo stabilimento del responsabile del trattamento nell'Unione Europea in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

- rappresentante: la persona fisica o giuridica stabilita nell'Unione Europea che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;
- norme vincolanti d'impresa: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;
- autorità di controllo: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR;
- autorità di controllo interessata: un'autorità di controllo interessata dal trattamento di dati personali in quanto: a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo; b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure c) un reclamo è stato proposto a tale autorità di controllo;
- trattamento transfrontaliero: a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione Europea ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione Europea, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;
- obiezione pertinente e motivata: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione Europea;

3. Principi, ambito di applicazione e destinatari del regolamento

1. Il presente documento si applica a tutti i trattamenti dei dati personali, automatizzati o effettuati manualmente, svolti dalla Sotacarbo S.p.A. in qualità di titolare. La Società si impegna a garantire e dimostrare che il trattamento dei dati avviene in maniera conforme a quanto previsto dalla normativa vigente e secondo i seguenti principi di liceità di trattamento:

- l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

- 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;
- il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
- il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito li titolare del trattamento;
- 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.
- il trattamento è limitato nel tempo a quanto necessario rispetto alle finalità per le quali sono trattati;
- I dati personali sono 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;
- il trattamento garantisce 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.

2. Le presenti indicazioni sono valide anche, per tuti quei trattamenti di cui Sotacarbo S.p.A. è nominata responsabile esterno da altri titolari, salvo la presenza di misure più restrittive in materia di protezione dei dati personali.
3. La stessa garanzia di protezione e di adozione di adeguate misure di sicurezza è altresì richiesta a quei soggetti terzi cui la società ha affidato l'incarico di gestire alcuni trattamenti. A tal fine il regolamento sul trattamento dei dati è disponibile presso i responsabili del trattamento nominati.
4. Il regolamento si applica ai dipendenti di Sotacarbo S.p.A. e ai collaboratori esterni a cui vengono assegnate particolari funzioni (RSPP, medico competente, responsabile dell'organismo di vigilanza, consulente del lavoro, ecc.).

4. Condizioni per il consenso

Le condizioni per il consenso che devono sussistere sono:

- qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali;
- se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro;
- l'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato e informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato;

- nel valutare se li consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

5. Organigramma e sistema di nomine e responsabilità

Al fine di garantire la tutela dei diritti delle persone fisiche relativamente al trattamento dei dati personali, la Società, nella figura del suo legale rappresentante, ha nominato il DPO e i referenti interni per il trattamento dei dati personali in relazione alla mansione svolta che potrebbe comportare il trattamento dei dati relativo alle persone fisiche. Di seguito si riportano i nominativi degli incaricati dal titolare del trattamento dei dati personali:

- Direttore Affari generali: Gianni Serra
- Responsabile amministrazione: Valentina Serra
- Responsabile trasparenza: Davide Marotto
- Data Protection Officer (DPO): Fabrizio Tedde
- Responsabile protocollo: Massimiliano Demurtas
- Incaricato rendicontazione progetti: Giovanni Perra
- Rappresentante dei lavoratori per la sicurezza: Ivo Puddu
- Addetta ai sistemi informatici: Elisabetta Fenu

5.1 Titolare del trattamento

Conformemente a quanto previsto dalla normativa, è titolare del trattamento la Sotacarbo S.p.A., nella persona del suo Amministratore Unico, e si impegna a:

- adeguare il proprio assetto organizzativo nel rispetto della normativa vigente in materia di protezione dei dati;
- adottare le modalità operative connesse con la gestione degli adempimenti e di trattamento dei dati;
- assumere le decisioni in ordine alle finalità, alle modalità del trattamento dei dati e agli strumenti utilizzati, ivi compreso li profilo della sicurezza, sia per i trattamenti svolti all'interno che all'esterno della propria struttura;
- individuare e designare i referenti/incaricati interni e responsabili esterni del trattamento dei dati, impartendo loro le relative istruzioni;
- vigilare sulla puntuale osservanza delle disposizioni e istruzioni impartite, anche nei confronti degli incaricati interni e dei responsabili del trattamento (esterni).

Essa, inoltre, si impegna a garantire l'esercizio dei diritti degli interessati e a tal scopo, ha implementato apposite procedure al fine di informare gli interessati dell'esistenza dei seguenti diritti:

- diritto di ottenere la conferma dell'esistenza o meno di dati personali che la riguardano e di averne accesso c.d. diritto all'accesso. In particolare l'interessato ha diritto di conoscere l'origine dei dati personali le finalità e modalità del trattamento; la logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; gli estremi identificativi del titolare, dei responsabili e del rappresentante designato; l'elenco dei soggetti o delle

categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati;
- diritto di ottenere l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati c.d. diritto alla rettifica:
- diritto di ottenere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati c.d. diritto alla cancellazione;
- diritto di limitare od opporsi, per motivi legittimi, al trattamento, rivolgendosi al personale espressamente incaricato c.d. diritto di opposizione.
- diritto alla portabilità dei dati
- diritto di non essere sottoposto a decisioni basate unicamente su trattamento automatizzato, inclusa la profilazione (art. 22 GDPR) che risulta essere particolarmente rilevante alla luce dell'introduzione di sistemi IA.

Al fine di esercitare i diritti sopra descritti, la Società si impegna a rispondere senza ritardo alle richieste presentate da parte dell'interessato ai Responsabili o agli Incaricati nominati, in forma orale o attraverso ulteriori idonei strumenti.

5.2.1 Posizione del responsabile della protezione dei dati (DPO)

- Il titolare del trattamento si assicura che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali;
- Il titolare del trattamento sostiene il responsabile della protezione dei dati nell'esecuzione dei compiti di cui la punto 6.2.2 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica;
- il titolare del trattamento si assicura che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento;
- gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento;
- il responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione Europea o degli Stati membri;
- il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi.
- In adempimento degli obblighi derivanti dalla L. 190/2012 e dal D.Lgs. 175/2016, la Società adotta il Piano Triennale per la Prevenzione della Corruzione e della Trasparenza (PTPCT). Il Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT) e il DPO si coordinano per la gestione dei trattamenti di dati personali connessi alle procedure di

appalto, alla gestione delle segnalazioni di illecito (whistleblowing ex D.Lgs. 24/2023) e alla pubblicazione nella sezione 'Amministrazione Trasparente'.

5.2.2 Compiti del responsabile della protezione dei dati (DPO)

Il responsabile della protezione dei dati è incaricato dei seguenti compiti:

a. informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione Europea o degli Stati membri relative alla protezione dei dati;
b. sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione Europea o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c. fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del GDPR in particolare può proporre al Titolare di procedere alla redazione di una DPIA ai sensi dell'art. 35 GDPR nei casi previsti dalla normativa, inclusi, a titolo esemplificativo: (i) trattamenti sistematici e su larga scala di dati particolari ex art. 9 GDPR; (ii) monitoraggio sistematico di aree accessibili al pubblico; (iii) utilizzo di nuove tecnologie. La DPIA è redatta dal DPO con il supporto dei referenti interni interessati, è approvata dal Titolare e conservata nel registro dei trattamenti. In caso di rischio residuo elevato non mitigabile, il Titolare effettua la consultazione preventiva del Garante ai sensi dell'art. 36 GDPR prima di avviare il trattamento;
d. cooperare con l'autorità di controllo;
e. fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del GDPR, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.
f. vigilare sull'effettivo funzionamento delle prescrizioni adottate dalla Società in materia di protezione dei dati personali;
g. effettuare audit in materia di privacy e controllare l'applicazione del principio di privacy by design e by default;
h. promuovere la cultura della protezione dei dati all'interno della Società e contribuire a dare attuazione a elementi essenziali del GDPR (es. principi fondamentali del trattamento, diritti degli interessati, privacy by design e by default, registro delle attività di trattamento, sicurezza dei trattamenti e data breach);
i. conservare e aggiornare l'elenco dei referenti interni, responsabili esterni e autorizzati al trattamento dei dati personali;
j. predisporre e attuare adeguati flussi di comunicazione da e verso i referenti interni, i responsabili esterni e gli autorizzati, inclusi gli alert/data breach di sistema;
k. fungere da punto di contatto per l'interessato relativamente a tutte le questioni inerenti li trattamento dei loro dati personali e all'esercizio dei loro diritti;
l. redigere una relazione annuale sulle proprie attività da sottoporre al titolare del trattamento dei dati personali;
m. tenere e aggiornare il registro dei trattamenti;

n. supportare i referenti, fornendo un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
o. informare tempestivamente li titolare in caso di data breach.

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

5.3 Incaricati/referenti interni del trattamento

L'incaricato/referente interno del trattamento dei dati è la persona nominata dal titolare al fine di garantire l'attuazione delle misure di sicurezza previste in materia di trattamento dei dati.
La persona preposta allo svolgimento della funzione viene individuata in quanto dotata di adeguate garanzie e soddisferà i seguenti punti:

- qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a referenti del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato;
- il referente del trattamento non ricorre a un altro referente senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il
- referente del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche;
- i trattamenti da parte di un referente del trattamento sono disciplinati da un atto giuridico (nomina) a norma del diritto dell'Unione Europea o degli Stati membri, che vincoli il referente del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. L'atto giuridico prevede, in particolare, che il referente del trattamento:
  a. tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione Europea o nazionale cui è soggetto li referente del trattamento;
  b. in tal caso, il referente del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
  c. adotti tutte le misure richieste ai sensi dell'articolo 32 del GDPR, in particolare garantisca: la pseudonimizzazione e la cifratura dei dati personali;
  d. la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
  e. la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
  f. una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;

g. tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
h. assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
i. su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione Europea o degli Stati membri preveda la conservazione dei dati;
j. metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di riservatezza e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato;
k. il referente del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione Europea, relative alla protezione dei dati;
l. se un referente del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, e considerato un titolare del trattamento in questione.

Inoltre, il referente del trattamento dovrà:

- redigere e aggiornare il registro delle attività di trattamento,
- segnalare al titolare e al DPO eventuali casi di data breach, segnalati da parte delle sue risorse o autonomamente individuati
- cooperare in caso di attività di controllo in ambito di trattamento dei dati personali da parte di strutture interne o esterne, fornendo eventuale documentazione richiesta e garantendo l'accesso ai locali
- informare il DPO dell'esistenza di un nuovo progetto che impatta sulla protezione dei dati, in applicazione del principio di privacy by design e by default
- Informare il DPO dell'esistenza di un nuovo trattamento per cui risulta necessario aggiornare il registro o modificarlo, in applicazione del principio di privacy by design e by default;
- informare il DPO della presenza di una nuova risorsa che tratta dati personali al fine di valutare la necessità di formazione in ambito privacy;
- segnalare casi di mancato rispetto delle disposizioni in tema di protezione dei dati al DPO
- proporre al titolare del trattamento dei dati la nomina di soggetti esterni quali responsabile del trattamento dei dati in relazione all'affidamento agli stessi di determinate attività;
- attuare gli obblighi di informazione ed acquisizione del consenso, quando richiesto, nei confronti degli interessati;
- garantire all'interessato che ne faccia richiesta l'effettivo esercizio dei diritti previsti dalla normativa di settore;
- distruggere i dati personali alla fine dei trattamenti degli stessi nei casi previsti dal regolamento secondo le procedure atte a garantire la sicurezza degli stessi e provvedere alle formalità di legge e agli adempimenti necessari anche mediante comunicazione al Garante della Privacy, se dovuta;

- comunicare immediatamente al titolare non oltre le **24 ore** successive al loro ricevimento, ogni richiesta, ordine o attività di controllo da parte del Garante o dell'Autorità Giudiziaria;
- osservare le procedure in materia di protezione dei dati personali adottate dal titolare;

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare allo stato non ha nominato alcun responsabile interno, ma esclusivamente autorizzati al trattamento.

5.4 Responsabile esterno del trattamento

Il responsabile esterno del trattamento dei dati è la persona nominata dal titolare al fine di garantire l'attuazione delle misure di sicurezza previste in materia di trattamento dei dati. Il responsabile esterno dovrà attuare le medesime azioni del referente/incaricato interno di cui al punto 6.3

5.5 Addetto ai sistemi informatici

L'addetto ai sistemi informatici è la figura professionale che, in ambito informatico, mantiene, configura e gestisce reti e apparati di telecomunicazione e di sicurezza.

5.6 Autorizzati al trattamento

Sono Autorizzati al trattamento dei dati personali i dipendenti autorizzati a trattare dati personali, sia in formato cartaceo che elettronico, strettamente necessari all'espletamento delle mansioni lavorative ad essi assegnate, coerentemente con le finalità istituzionali del Titolare definite nel presente regolamento.
In conformità agli artt. 24, 32 e 29 del GDPR, l'Autorizzato è tenuto ad attenersi alle istruzioni e alle pratiche di buona condotta in ambito informatico previste nei relativi regolamenti aziendali e nella vigente normativa in campo Privacy e sicurezza informatica. Secondo tali principi e in accordo con quanto previsto all'art. 28 punto 3, e all'art. 29 la persona "autorizzata al trattamento dei dati personali" è debitamente informata ed istruita al fine di mettere in atto comportamenti che assicurino l'adeguato livello di sicurezza e riservatezza commisurato al "valore del dato" e ai conseguenti rischi.
All'interno della struttura aziendale sono Autorizzati al trattamento i dipendenti svolgenti le seguenti funzioni:

- RUP, Responsabili di fase, DEC, Direttore dei lavori nominati internamente e tutte quelle figure che nella gestione di un appalto si trovino a dover trattare dati personali;
- Responsabile ufficio acquisti
- Responsabile ufficio del personale
- Personale amministrativo che nello svolgimento dei propri compiti debba trattare dati personali
- Personale addetto alla selezione del personale
- Personale tecnico che nell'ambito dei compiti assegnati debba trattare dati personali

Gli autorizzati al trattamento vengono nominati mediante apposito atto scritto, *Nomina autorizzato al trattamento dati personali MOD.A.T.D.P.*, che stabilisce l'ambito del trattamento, le istruzioni

operative e le misure di sicurezza da adottare per il trattamento, gli obblighi a cui l'Autorizzato deve rispondere e le sanzioni previste laddove si contravvenga a tali obblighi.

6. Impegno alla riservatezza

La Società, in qualità di titolare del trattamento dei dati, si impegna a garantire la riservatezza, conformemente alle procedure interne e la confidenzialità delle informazioni e dei dati degli interessati acquisiti nel corso della propria attività.
A tal scopo, i dati e le informazioni raccolte durante lo svolgimento dell'incarico sono trattati per:

- finalità strettamente connesse ala propria attività lavorativa;
- finalità connesse agli obblighi previsti da leggi, regolamenti e normativa comunitaria nonché da disposizioni impartite ad autorità a ciò legittimate dalla legge.

In relazione alle indicate finalità il trattamento dei dati avverrà in modo da garantire la sicurezza e la riservatezza e potrà essere effettuato attraverso strumenti manuali, informatici e telematici atti a memorizzare, gestire e trasmettere i dati stessi nel rispetto delle misure di sicurezza previste dal DL. gs 196/2003 e dal GDPR. Tutti gli amministratori e dipendenti di Sotacarbo S.p.A. sono tenuti al segreto in conformità all'art. 2105 c.c. (obbligo di fedeltà e riservatezza dei dipendenti) e, per gli amministratori, alle disposizioni dello statuto sociale e alle norme applicabili in materia di doveri degli organi gestori.
Tutti i dati e le informazioni acquisite, in aggiunta alle comunicazioni previste nei confronti di soggetti e organi che hanno responsabilità di direzione, supervisione e controllo potranno essere comunicati esclusivamente a:

- autorità di vigilanza, italiane o estere, nei casi e con le limitazioni previste dalla legge;
- autorità amministrativa, giudiziaria e fiscale, nei casi e con le limitazioni previsti dalla legge;
- fornitori di servizi e/o consulenti tecnico-informatici, anche in paesi terzi non comunitari, unicamente per esigenze tecniche connesse all'utilizzo da parte del titolare di sistemi e/o applicazioni strumentali nell'esecuzione degli obblighi contrattuali assunti nell'ambito dell'incarico in oggetto e dei correlati obblighi di legge, fermo restando che il ricorso a tali soggetti avverrà previo impegno da parte loro a rispettare tutte le prescrizioni in materia di sicurezza dei dati previste dal DL.gs 169/2003 e dal GDPR.

La Società si impegna a garantire gli standard indicati nelle disposizioni in oggetto nei confronti dei terzi con la medesima diligenza e livello di protezione utilizzati per la sicurezza e la riservatezza dei propri dati.

7. Registro delle attività di trattamento dei dati personali

In attuazione del presente regolamento il titolare del trattamento ha deciso di adottare un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tute le seguenti informazioni:

a. il nome e i dati di contatto del titolare del trattamento e del responsabile della protezione dei dati (DPO);
b. le finalità del trattamento;
c. una descrizione delle categorie di interessati e delle categorie di dati personali;

d. le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
e. ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione Internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per trasferimenti di cui al secondo comma dell'articolo 49 del GDPR, la documentazione delle garanzie adeguate;
f. ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati
g. ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1 del GDPR.

Ogni referente/incaricato interno e responsabile esterno del trattamento tiene un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:

a. Il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
b. le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
c. ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione Internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per trasferimenti di cui al secondo comma dell'articolo 49 del GDPR, la documentazione delle garanzie adeguate:
d. ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1 del GDPR.

I registri sono tenuti in forma scritta, anche in formato elettronico. Su richiesta, il titolare del trattamento o il responsabile esterno del trattamento mettono il registro a disposizione dell'autorità di controllo.

7.1 Dati dei dipendenti dei collaboratori e dei componenti degli organi aziendali

Sotacarbo S.p.A. al fine di adempiere ai propri obblighi di gestione del personale, raccoglie i dati dei componenti degli organi aziendali e dei propri dipendenti, informandoli dei propri diritti.

- In particolare, il trattamento dei dati delle suddette categorie è previsto per finalità amministrativo - contabili, quali ad esempio:
- gestione delle buste paga, gestione delle trasferte, promozioni e premi;
- pianificazione degli avanzamenti di carriera;
- gestione dei piani di formazione;
- gestione dei dati anagrafici per finalità di legge (ad es. in adempimento del d.lgs. 81/08 in tema di sicurezza sul lavoro).

Con riferimento al trattamento dei dati del personale, Sotacarbo S.p.A. si impegna a verificare l'acquisizione del consenso al trattamento dei dati e a fornire adeguata informativa. (Allegato 1- registro dei trattamenti di Sotacarbo S.p.A.).

7.2 Dati dei fornitori

Sotacarbo S.p.A. per mezzo dei propri referenti o autorizzati, può raccogliere i dati personali dei fornitori, al fine di perfezionare accordi contrattuali. I dati personali dei fornitori potranno essere trattati nell'ambito della normale attività di Sotacarbo S.p.A. per le seguenti finalità:

- fornire i servizi richiesti e gestire i rapporti con i fornitori;
- adempiere ad obblighi previsti da un regolamento o dalla normativa comunitaria nonché per osservare disposizioni impartite dalle pubbliche autorità ed organi di vigilanza e controllo a ciò legittimati dalla legge. In tal caso li conferimento dei dati personali è necessario e obbligatorio e per il trattamento di tali dati non è richiesto il consenso.

7.3 Dati dei terzi

Durante lo svolgimento dell'attività, Sotacarbo S.p.A. può venire a conoscenza di dati che riguardano terzi, ovvero fornitori, collaboratori ecc.
In tali casi Sotacarbo S.p.A. si impegna a sottoscrivere apposita clausola o accordo al fine di garantire la corretta applicazione delle presenti indicazioni anche nei rapporti con i terzi.

7.4 Coordinamento tra obblighi di trasparenza e protezione dei dati personali

In qualità di società a partecipazione pubblica, Sotacarbo S.p.A. è soggetta agli obblighi di pubblicazione di cui al D.Lgs. 33/2013 e ss.mm.ii. (c.d. Decreto Trasparenza). Il Responsabile della Trasparenza e il DPO si coordinano al fine di: (i) garantire che le pubblicazioni nella sezione 'Amministrazione Trasparente' del sito istituzionale avvengano nei limiti strettamente necessari, senza eccedere i dati richiesti dalla legge; (ii) gestire le istanze di accesso civico generalizzato (FOIA) bilanciando il diritto di accesso con la tutela dei dati personali di terzi, in conformità alle Linee guida del Garante e dell'ANAC; (iii) redigere un'apposita voce nel registro dei trattamenti dedicata ai trattamenti derivanti dagli obblighi di trasparenza.

8. Misure di sicurezza e relativi controlli

8.1 La gestione della sicurezza: ruoli e responsabilità

La responsabilità dell'attività di impostazione e coordinamento dei sistemi che garantiscono la sicurezza e la tutela di tutti i dati oggetto di trattamento aziendale sia da un punto di vista logico che fisico, la loro gestione diretta o tramite fornitori, sono in carico all'addetto sistemi informatici.
L'addetto sistemi informatici segue i seguenti criteri generali:

- in base alle figure professionali presenti in azienda, vengono definiti i profili standard da assegnare agli utenti con le autorizzazioni necessarie all'espletamento delle rispettive mansioni definite per ruoli e competenze;

- la validità delle richieste di accesso alla rete è verificata automaticamente dal sistema stesso prima di consentire l'accesso ai dati, tramite un sistema di autenticazione costituito da user-ID e password.

Sotacarbo S.p.A., in qualità di titolare del trattamento dei dati, è tenuta a proteggere i dati personali trattati in modo sicuro.
I dati in formato elettronico sono archiviati preferibilmente su Cartelle in Cloud con protezione adeguata. L'archiviazione su server o PC privi di cifratura dei dischi è consentita esclusivamente previa valutazione documentata del rischio, redatta dall'addetto ai sistemi informatici e approvata dal DPO, che attesti l'adeguatezza delle misure alternative adottate (controllo degli accessi fisici e logici, autenticazione forte, sistemi di rilevazione delle intrusioni). Tale valutazione è allegata al registro dei trattamenti e aggiornata con cadenza annuale.

8.2 Misure per garantire l'integrità a protezione dell'accesso ai dati

Sono le misure di sicurezza volte a minimizzare i rischi che le informazioni siano rivelate o modificate senza autorizzazione, ovvero perse o alterate accidentalmente o intenzionalmente.
Il sistema in atto prevede un sistema di autenticazione, basato su codice identificativo e password individuale segreta, per assicurare che la persona che accede al sistema sia identificata con certezza, nonché un sistema di autorizzazione, che prevede che a ciascuna persona che accede al sistema sia assegnato un profilo di accesso che definisce i dati ai quali l'utente è autorizzato ad accedere e, ove applicabile, le operazioni che per ciascun dato o gruppo di dati è autorizzato ad eseguire (consultazione, inserimento, modifica, cancellazione).
Nessun dipendente di Sotacarbo S.p.A. è amministratore dei sistemi informatici forniti in dotazione, eccetto li DPO e l'addetto sistemi informatici.

8.3 Sicurezza della postazione di lavoro

Lo scopo di questa politica è di stabilire i requisiti minimi per prevenire eventi di data breach e responsabilizzare i dipendenti aziendali. Di seguito sono elencati i comportamenti da applicare:

- i dipendenti sono tenuti a garantire che tutte le informazioni sensibili o confidenziali in formato elettronico o cartaceo siano messe al sicuro nella propria postazione di lavoro, in particolare alla fine della giornata lavorativa e in caso di assenza prolungata;
- i computer devono essere bloccati quando le postazioni di lavoro non sono occupate;
- tutti i computer devono essere spenti alla fine della giornata lavorativa;
- qualsiasi informazione e/o dato riguardante persone fisiche deve essere rimosso dalla scrivania e chiuso a chiave in un cassetto quando la postazione di lavoro non è occupata e alla fine della giornata lavorativa;
- le cartelle contenenti informazioni riservate e/o dati riguardanti persone fisiche devono essere tenute chiuse e bloccate quando non utilizzate;
- le chiavi utilizzate per accedere alle informazioni riservate e/o ai dati riguardanti persone fisiche non devono essere lasciate su una scrivania non presidiata;
- i pc portatili devono essere conservati in un cassetto o armadio chiuso a chiave se non utilizzati
- le password non possono essere lasciate su note adesive attaccate sopra o sotto un computer, né possono essere lasciate per iscritto su una postazione accessibile:

- le stampe contenenti informazioni riservate e/o dati riguardanti persone fisiche devono essere immediatamente rimosse dalle stampanti;
- al momento dello smaltimento, i documenti riservati o contenenti dati particolari/sensibili devono essere triturati nei distruggi documenti appositi;
- le lavagne contenenti informazioni riservate e/o dati riguardanti persone fisiche devono essere cancellate;
- I dispositivi portatili come computer portatili, smartphone o tablet non devono mai essere lasciati sbloccati e incustoditi:
- tutti i dispositivi di archiviazione di massa come CDROM, DVD o chiavi USB contenenti informazioni riservate e/o dati riguardanti persone fisiche devono essere conservati in cassetti chiusi a chiave.

8.4 Misure per garantire la disponibilità dei dati

Sono le attività volte a ridurre i rischi di indisponibilità (parziale o totale) nell'accesso al sistema informatico di Sotacarbo S.p.A.

8.4.1 Processo di assunzione dei dipendenti

Nel contesto di assunzione di una nuova risorsa in Sotacarbo S.p.A., li titolare invierà una mail almeno 15 giorni prima della data di ingresso della risorsa al responsabile d'area per la creazione dell'utenza sull'applicativo gestionale Zucchetti e per la preparazione del PC e di eventuale telefono aziendale. Questi ultimi vengono consegnati al momento dell'Ingresso della nuova risorsa.
Tutti i dipendenti hanno un unico ID di accesso su Zucchetti (tramite id e password) con cui effettueranno l'acceso al sistema per la richiesta di ferie, permessi e missioni. I dipendenti sono inoltre dotati di un cartellino personale per la rilevazione delle presenze. Sia le password che il cartellino sono strettamente personali ed è vietato condividerli con uno o più soggetti.
Sotacarbo S.p.A. può modificare i diritti di accesso ai servizi e ai sistemi in qualsiasi momento e per qualsiasi ragione.
Tutti i dipendenti di Sotacarbo S.p.a. non sono amministratori dei dispositivi rilasciati in dotazione eccetto il DPO e l'addetto sistemi informatici.

8.4.2 Processo di dimissione del dipendente

Nel caso di dimissioni di una risorsa da Sotacarbo S.p.A., il titolare informerà tramite mail almeno 15 giorni prima della data di cessazione del rapporto di lavoro il responsabile competente, che avviserà l'addetto sistemi informatici per la disabilitazione dell'utenza e per la riconsegna del PC e dell'eventuale telefono aziendale. L'addetto sistemi informatici disabiliterà immediatamente tutti i diritti di accesso del dipendente sui sistemi aziendali compresa la mail e il cloud aziendale e provvederà alla dismissione dell'utenza assegnata e della relativa licenza software.

8.4.3 Dismissione dei dispositivi utilizzati dagli utenti di Sotacarbo S.p.A.

Tutti i dispositivi di Sotacarbo S.p.A., rilasciati in dotazione ai dipendenti, vengono formattati a seguito delle dimissioni degli stessi al fine di rimuovere tutti i dati personali contenuti al loro interno.

Tutti i dipendenti di Sotacarbo S.p.A. sono, quindi, tenuti ad assicurarsi che venga correttamente eseguito il passaggio di consegne tra i colleghi del gruppo affinché venga assicurata la continuità dei servizi erogati. I sistemi informatici dismessi quali: pc, tablet e telefoni cellulari non potranno essere ceduti anche gratuitamente a terzi ma dovranno essere opportunamente distrutti per evitare il recupero totale o parziale delle informazioni in questi contenute.

8.5 Livelli di sicurezza

Il DPO per valutare la sicurezza del sistema informatico in azienda opererà, coadiuvato dall' addetto sistemi informatici, le seguenti azioni:

- assegnerà agli utenti le autorizzazioni necessarie all'espletamento delle proprie mansioni (definite per ruoli e competenze) in relazione alle effettive esigenze operative. A tal scopo viene limitato l'accesso logico a reti, sistemi e basi dati;
- indicherà le modalità di gestione delle password che indicano la lunghezza, la complessità, la durata, la conservazione sicura. Pertanto le password dovranno avere una lunghezza minima di 8 caratteri e dovrà essere composta da almeno un numero, una lettera maiuscola, una minuscola e un carattere speciale (per esempio: $, %, @, &, ecc.).
- dovrà adottare, entro 6 mesi dall'entrata in vigore del regolamento, tecniche e metodologie per la verifica nel continuo dell'utilizzo dei sistemi applicativi e per il controllo del traffico di rete generato al fine di garantire pronto intervento in caso di attività anomale
- controllerà periodicamente le misure di sicurezza, anche attraverso esercizi di penetration test, al fine di prevenire ipotesi di Data Breach;
- organizzerà sessioni di formazione dei dipendenti al fine di metterli a conoscenza dei rischi in materia di privacy.
- modificherà i regolamenti interni al fine di renderli aderenti alla normativa sulla privacy;
- controllerà periodicamente l'adeguatezza, l'affidabilità complessiva e la tutela del sistema informativo.

9. Informazione e formazione dei destinatari

L'obiettivo di garantire un corretto trattamento dei dati, conforme ai requisiti previsti dalla normativa, viene raggiunto dalla Società anche e soprattutto grazie alla particolare attenzione risposta nei confronti della formazione del proprio personale.
A tal proposito, fin dal momento di ingresso di una nuova risorsa, Sotacarbo S.p.A. presenta a quest'ultima il regolamento aziendale sul trattamento dei dati, nonché le comunica eventuali aggiornamenti con e-mail inviata a tutti i dipendenti. Questo regolamento viene inviato via e-mail a tutti i dipendenti e affisso nella bacheca aziendale.
Allo scopo di formare i referenti dei trattamenti, la Società:

- adotta un piano formativo con l'obiettivo di alfabetizzazione in materia di protezione dei dati personali destinato a tutto il personale della società;
- prevede l'erogazione di un modulo relativo alla formazione sulla privacy all'interno dei corsi organizzati all'atto dell'ingresso in servizio in Sotacarbo S.p.A. o anche al momento del cambio di mansione qualora tale cambio preveda l'utilizzo di un nuovo applicativo, sistema o software all'interno della quale vengono trattati dati personali;

- prevede un piano di formazione programmato con cadenza annuale sulla formazione erogata in ambito della privacy a tutti i dipendenti della società:
- conserva la documentazione distribuita e la modulistica attestante la partecipazione agli interventi formativi.

La formazione dei referenti e degli incaricati riguarda in particolare:

- aspetti della disciplina di protezione dei dati personali, in ambito generale ed ambito specifico i rischi che minacciano i dati;
- le conseguenze derivate dalla violazione di dati personali (Data Breach);
- le procedure da seguire in caso di Data Breach;
- le misure disponibili per evitare eventi di Data Breach;
- aspetti della disciplina di protezione dei dati personali, in ambito generale ed ambito specifico
- training per aggiornare li personale sulle misure adeguate di sicurezza e protezione dei dati personali adottate dal titolare del trattamento;

La formazione deve essere:

- adeguata al proprio sistema di trattamenti dei dati:
- capace di trasmettere agli incaricati e responsabili del trattamento misure adeguate di sicurezza e protezione dei dati personali adottate dal titolare;
- documentabile, in quanto la formazione dell'avvenuto training è parte integrante del regolamento sul trattamento dei dati personali di Sotacarbo S.p.A.

10. Notifica di una violazione dei dati personali all'autorità di controllo (Data Breach)

- In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 del GDPR senza ingiustificato ritardo e, ove possibile entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo;
- la violazione sarà comunicata tramite i moduli allegati al presente regolamento all'interessato (allegato 2) e all'autorità di controllo (allegato 3);
- il DPO terrà un registro dei data breach (allegato 4);
- il DPO, il referente/incaricato interno o il responsabile esterno del trattamento informa il titolare del trattamento non appena essere venuto a conoscenza della violazione;
- la notifica deve almeno contenere i seguenti punti:

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

- Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo;
- il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo del regolamento.

11. Comunicazione di una violazione dei dati personali all'interessato

1 La violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, viene comunicata dal titolare del trattamento all'interessato tempestivamente con un linguaggio semplice e chiaro e contiene le informazioni e le misure di cui all'articolo 33, paragrafo 3 lettere b), c) e d) del GDPR;

2 Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:

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

12. Non osservanza della normativa societaria

Il dipendente che viola le norme di comportamento indicate nel presente regolamento sul trattamento dei dati personali potrà essere soggetto ad azioni disciplinari, fino al licenziamento.

13. Aggiornamento

Il presente regolamento verrà aggiornato laddove dovessero subentrare aggiornamenti di carattere normativo, tecnologico o che comportino modifiche sostanziali alle procedure e alle misure in esso indicate. Tale aggiornamento sarà a cura del DPO in coordinamento con quanti altri possano essere coinvolti.

14. Coordinamento con gli altri regolamenti

Il presente regolamento si intende da applicarsi coordinatamente con il Regolamento per l'utilizzo aziendale dell'intelligenza artificiale generativa (GenAI) in merito agli obblighi specifici per il deployer.

15. Entrata in vigore

Il presente regolamento entra in vigore con la pubblicazione sul sito web aziendale.

Carbonia, 31/07/2026

Ing. Mario Porcu
Amministratore Unico Sotacarbo SpA

Firmato digitalmente da:
MARIO PORCU
31/07/2026 14:45