SOTACARBO

SUSTAINABLE ENERGY
RESEARCH CENTRE

Regolamento Aziendale n.10 per la tutela della privacy ai sensi del Regolamento UE n.679/2016 (GDPR) e del D.Lgs n.196 del 30.06.2003 armonizzato dal D.Lgs 101/2018

SOTACARBO
SUSTAINABLE ENERGY RESEARCH CENTRE

Sommario

1. Introduzione

Lo scopo del presente documento è definire le procedure per adempiere ai dettami del D.Lgs. n. 196 del 30.06.2003 (codice per la protezione dei dati personali – c.d. Codice della Privacy) e del Regolamento UE n. 679 del 2016 (General Data Protection Regulation – c.d. GDPR), in materia di privacy aziendale, ovvero individuare le disposizioni operative interne volte a disciplinare il trattamento dei dati personali effettuato dalla Società.

In essa sono quindi disciplinati i ruoli e le responsabilità nonché gli adempimenti da seguire in materia di protezione dei dati personali anche con riferimento alle decisioni e ai provvedimenti emessi dall'Autorità Garante per la protezione dei dati personali.

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 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;
- Soggetto interno designato: il dipendente incaricato dal titolare del trattamento dati relativo alla sua funzione secondo l'articolo 2-quaterdecies del D.Lgs. 196/03;
- 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 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 il 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 sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- dati biometrici: i dati personali ottenuti da un trattamento tecnico specifico 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, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione 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 o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione 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 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;
- impresa: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;
- gruppo imprenditoriale: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;
- 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 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, 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;
- servizio della società dell'informazione: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio;
- organizzazione internazionale: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

3. Principi, ambito di applicazione e destinatari del regolamento

Il presente documento si applica a tutti i trattamenti dei dati personali, automatizzati o svolti manualmente, effettuati dalla Sotacarbo S.p.A. in qualità di titolare.

Il presente regolamento interno è operativo dal 1 aprile 2019 tramite deliberazione del Consiglio di Amministrazione del 27.03.2019.

La Società si impegna a garantire e dimostrare che il trattamento dei dati avviene in maniera conforme a quanto previsto dalla normativa e secondo i seguenti principi di liceità di trattamento (art.6 del Regolamento):

- 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 il 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.

Le presenti indicazioni sono valide anche, per tutti 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.

La stessa garanzia di protezione e di adozione di adeguate misure di sicurezza è richiesta altresì a quei soggetti terzi ai quali la società ha affidato l'incarico della gestione di alcuni trattamenti. A tal fine il regolamento sul trattamento dei dati è disponibile presso i designati interni del trattamento nominati.
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 per l'elaborazione delle paghe, 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 è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato;
- nel valutare se il 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. Oggetto e modalità di applicazione

Oggetto del presente regolamento è il trattamento dei dati personali effettuato da Sotacarbo S.p.A..
Sono esclusi dall'ambito di applicazione i trattamenti dei dati personali effettuati dai lavoratori per fini esclusivamente personali e nei casi in cui i dati non sono destinati ad una comunicazione sistematica o alla diffusione anche se utilizzati ai fini di esigenze di lavoro (ad esempio, rubrica personale su telefono fisso o mobile ed utilizzata solo ed esclusivamente dall'utente).

6. 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 soggetti interni e esterni designati al trattamento dei dati personali in relazione alla mansione svolta che potrebbe comportare il trattamento dei dati relativo alle persone fisiche. In allegato 1 si riportano i nominativi dei soggetti designati dal titolare del trattamento dei dati personali.

6.1. Titolare del trattamento

Conformemente a quanto previsto dalla normativa, è titolare del trattamento la Sotacarbo S.p.A., nella persona del suo legale rappresentante, e si impegna a mettere in atto tutte le misure tecniche ed organizzative necessarie per garantire che il trattamento è effettuato conformemente al GDPR (articolo 24 del Regolamento). In particolare:

- 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 ed il trattamento dei dati;
- assumere le decisioni in ordine alle finalità, alle modalità del trattamento dei dati e agli strumenti utilizzati, ivi compreso il profilo della sicurezza, sia per i trattamenti svolti all'interno che all'esterno della propria struttura;
- individuare e designare i soggetti interni designati 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);
- nominare il responsabile della protezione dei dati (RPD)/data protection officer (DPO).

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 (art.15 del Regolamento). 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 (art.16 del Regolamento):
- 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 (art.17 del Regolamento);
- diritto di limitare od opporsi, per motivi legittimi, al trattamento, rivolgendosi al personale espressamente incaricato; c.d. diritto di opposizione (art.21 del Regolamento).

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.

6.2. Responsabile della protezione dei dati (RPD) o data protection officer (DPO)

Il titolare del trattamento ha designato un responsabile della protezione dei dati in quanto la Sotacarbo SpA è equiparabile ad un organismo pubblico (art. 37 comma 3 del Regolamento). Comunque si precisa che la Sotacarbo SpA non ha per finalità il trattamento dei dati personali ma che tratta quella tipologia dei dati necessari alla propria attività istituzionale.

6.2.1. Posizione del responsabile della protezione dei dati (art.38 del Regolamento)

- 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 al 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 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.

6.2.2. Compiti del responsabile della protezione dei dati (art.39 del Regolamento)

Il responsabile della protezione dei dati è incaricato almeno 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 o degli Stati membri relative alla protezione dei dati;
b. sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione 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 Regolamento;
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 Regolamento, 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 Regolamento (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 designati interni, responsabili esterni e autorizzati al trattamento dei dati personali;
j. predisporre e attuare adeguati flussi di comunicazione da e verso i designati 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 il 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. coadiuvare il titolare nel tenere e aggiornare il registro dei trattamenti;
n. supportare i designati interni, fornendo un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
o. informare tempestivamente il 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.

6.3. Soggetti interni designati al trattamento (D.Lgs. 196/03 – art.2 quaterdecies)

Il soggetto interno designato al 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 designata 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 designati al trattamento che presentino garanzie sufficienti per mettere in atto

misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato;

- i trattamenti da parte di un designato al trattamento sono disciplinati da un atto giuridico (nomina) a norma del diritto dell'Unione o degli Stati membri, che vincoli il designato interno al 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. L'atto giuridico prevede, in particolare, che il referente del trattamento:
  - tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il designato interno del trattamento; in tal caso, il designato interno 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;
  - adotti tutte le misure indicate dal titolare per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
  - tenendo conto della natura del trattamento, assista il titolare del trattamento al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
  - assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli dal 32 al 34 del Regolamento, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
  - 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;
  - il designato interno al trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il Regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati;
- se un designato interno al trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, potrà essere oggetto di provvedimenti disciplinari.

Inoltre, il designato al trattamento dovrà:

- coadiuvare il titolare nel redigere e aggiornare il registro delle attività di trattamento (art.30 GDPR);
- segnalare al titolare e al DPO eventuali casi di data breach (artt. 33 e 34 del Regolamento);
- cooperare in caso di attività di controllo in ambito 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 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;
- coadiuvare il titolare del trattamento nell'attuare gli obblighi di informazione ed acquisizione del consenso, quando richiesto, nei confronti degli interessati;
- coadiuvare il titolare del trattamento nel 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, secondo le procedure atte a garantire la sicurezza degli stessi;
- osservare le procedure in materia di protezione dei dati personali adottate dal titolare.

6.4. Responsabile del trattamento (art.28 del Regolamento)

Il responsabile 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 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 del trattamento è designato allo svolgimento delle funzioni indicate nell'articolo 28 del Regolamento e viene individuato in quanto dotato 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 responsabili 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 Regolamento e garantisca la tutela dei diritti dell'interessato;
- i trattamenti da parte di un Responsabile del trattamento sono disciplinati da un atto giuridico (nomina) a norma del diritto dell'Unione o degli Stati membri, che vincoli il designato al 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:
  - tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il Responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
  - adotti tutte le misure richieste ai sensi dell'articolo 32 del GDPR, in particolare garantisca: la pseudonimizzazione e la cifratura dei dati personali; la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
  - 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;
  - assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli dal 32 al 34 del Regolamento, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
  - 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 o degli Stati membri preveda la conservazione dei dati;
  - 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;

  - il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il Regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati;
- se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione.

Inoltre, il responsabile del trattamento dovrà:
- in accordo con il titolare, redigere e aggiornare il registro delle attività di trattamento (art.30 del Regolamento);
- segnalare al titolare e al DPO eventuali casi di data breach, segnalati da parte delle sue risorse o autonomamente individuati (artt. 33 e 34 del Regolamento);
- cooperare in caso di attività di controllo in ambito 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 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 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 ha deciso di non nominare alcun responsabile interno.

6.5. Amministratore di sistema

La figura professionale che, in ambito informatico, mantiene, configura e gestisce reti e apparati di telecomunicazione di sicurezza è nominata amministratore di sistema.
L'attribuzione delle funzioni di amministratore di sistema avviene previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
La nomina ad amministratore di sistema deve essere individuale, formalizzata, con l'indicazione analitica degli ambiti di applicazione di operatività consentiti in base al profilo di autorizzazione assegnato.
In generale, l'amministratore di sistema ha le seguenti responsabilità:
- sovraintendere alle risorse dei sistemi computerizzati al fine di consentirne una corretta ed efficiente utilizzazione;

- sovraintendere all'acquisto delle apparecchiature informatiche Societarie che vada ad impattare sulla sicurezza della rete LAN interna al fine di consentirne una corretta ed efficiente utilizzazione;
- in accordo con il titolare e il DPO, fornire guida e supporto ai soggetti interni designati in merito al trattamento informatico dei dati personali;
- amministrare e gestire la sicurezza informatica;
- nell'ambito delle responsabilità assegnate, effettuare periodici controlli e verifiche tecniche, anche nei riguardi dei soggetti interni designati in merito a quanto previsto dal presente regolamento;
- sopraintende alla manutenzione del sistema. Per manutenzione s'intende non soltanto l'intervento tecnico diretto ad eliminare eventuali problemi hardware, ma anche gli interventi volti alla ricostruzione di archivi che dovessero in qualche modo risultare danneggiati o corrotti oltre all'intervento tecnico diretto ad eliminare eventuali avarie al software di sistema e all'applicativo utilizzato;
- per poter svolgere funzioni, allo stesso vengono concesse dal titolare le "autorità di sistema", che consistono nell'assegnazione di attributi, privilegi, o accessi che consentono la gestione delle "risorse critiche del sistema operativo", ovvero degli oggetti informatici necessari al funzionamento dei sistemi e del servizio di elaborazione dati (es. log di sistema, tabella di servizio, cataloghi dei dati, ecc.).

7. 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 alla propria attività lavorativa;
- finalità connesse agli obblighi previsti da leggi, regolamenti e normativa comunitaria nonché da disposizioni impartite da 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 Regolamento Europeo n.679/16 (GDPR). Tutti gli amministratori e dipendenti di Sotacarbo S.p.A. sono tenuti al segreto professionale previsto dall'art. 2105 del codice civile (dovere di fedeltà) e la cui violazione importa responsabilità disciplinare (art.2106 del c.c.).

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 Regolamento.

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.

8. Registro delle attività di trattamento dei dati personali (art.30 del Regolamento)

In attuazione del presente regolamento il titolare del trattamento ha deciso di adottare un registro delle attività di trattamento svolte sotto la propria responsabilità ed è coadiuvato dai designati interni per la sua compilazione. Tale registro contiene tutte 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 i 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 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 i 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 Regolamento.

I registri sono tenuti in forma scritta e/o in formato elettronico.

Su richiesta, il titolare del trattamento o il responsabile esterno del trattamento mettono il registro a disposizione dell'autorità di controllo.

8.1. 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;
- piano della performance e progressione 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).
- Dati sanitari (nelle disponibilità del solo medico competente)

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.

8.2. 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 il conferimento dei dati personali è necessario e obbligatorio e per il trattamento di tali dati non è richiesto il consenso;

8.3. 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.

8.4. Dati derivanti da curricola di candidati finalizzati all'assunzioni inviati in relazione a specifici bandi

Durante i processi selettivi di nuovo personale la Sotacarbo dovrà gestire i curricola inviati dai candidati. Questi dovranno essere custoditi in armadi chiusi a chiave o in computer protetti da password a cura del responsabile del protocollo che dovrà renderli disponibili solamente alla commissione incaricata della selezione previa firma di un'assunzione di responsabilità e presa visione del seguente regolamento.

8.5. Dati derivanti da curricola inviati spontaneamente da possibili candidati

In Società potrebbero arrivare curricola inviati spontaneamente dai candidati e non connessi ad alcun bando pubblicato dalla Sotacarbo. I curricola e quindi i dati in essi presenti dovranno essere conservati a cura del responsabile del protocollo in armadi opportunamente confinati e su supporti informatici ad accesso bloccato. All'atto delle attività di selezione (art.111 bis del D.Lgs. 196/03), bisognerà far firmare un modulo di informazione sulla privacy strutturato secondo l'art. 13 del Regolamento. I dati presenti nei curricola saranno utilizzati per i soli fini di selezione del personale e saranno conservati per un massimo di un anno.

8.6. Dati provenienti da terzi

La Sotacarbo potrebbe avvalersi di società esterne per il reclutamento del personale, in questo caso al candidato, all'atto delle attività di selezione, bisognerà far firmare un modulo di informazione sulla privacy strutturato secondo l'art. 14 del Regolamento. I dati presenti nei curricola saranno utilizzati per i soli fini di selezione del personale e saranno conservati per un massimo di un anno

9. Misure di sicurezza e relativi controlli

9.1. 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'amministratore di sistema.
L'amministratore di sistema 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 possono essere archiviati su: Cartelle in Cloud, cartelle su Server non cifrato, cartelle all'interno di PC non cifrato con password di complessità elevata.

9.2. 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 il titolare, il DPO e l'amministratore di sistema.

9.3. 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 della Sotacarbo SpA.
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 aziendali 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.

9.4. 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..

9.4.1. Processo di assunzione dei dipendenti

Nel contesto di assunzione di una nuova risorsa in Sotacarbo S.p.A., il titolare invierà una mail almeno 15 giorni prima della data di ingresso della risorsa al responsabile d'area per la creazione dell'utenza nel programma HR 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 nel programma HR (tramite id e password e codice identificativo) con cui effettueranno l'acceso al sistema per la richiesta di ferie, permessi e missione e per la compilazione del proprio timesheet. Il codice identificativo verrà utilizzato per la rilevazione delle presenze. Sia le password che il codice identificativo 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 titolare, il DPO e l'amministratore di sistema.

9.4.2. 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 di area, che avviserà l'amministratore di sistema per la disabilitazione dell'utenza e per la riconsegna di tutte le apparecchiature elettroniche in dotazione (PC, notebook, tablet e aziendale). L'amministratore di sistema disabiliterà immediatamente tutti i diritti di accesso del dipendente sui sistemi aziendali compresa la mail e il cloud aziendale.

9.4.3. 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 team 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.

9.4.4. Accesso ai dati contenuti nei dispositivi informatici in dotazione ai dipendenti

In caso di impedimento e/o prolungata assenza dell'incaricato o di indispensabile ed indifferibile intervento per necessità di operatività e di sicurezza del sistema il titolare può disporre dei dati e degli strumenti elettronici. L'amministratore di sistema, su indicazione scritta del titolare, potrà accedere ai computer aziendali in assenza del lavoratore e successivamente darne ad esso comunicazione per iscritto.

9.5. Livelli di sicurezza

Il titolare per valutare la sicurezza del sistema informatico in azienda opererà, coadiuvato dall'amministrazione di sistema e dal DPO, 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 dove possibile un carattere speciale (per esempio: £, $, %, @, &, ecc.), dovranno essere cambiate ogni 6 mesi e conservate in luogo sicuro (3 mesi se i dati contenuti nei sistemi appartengono alle categorie particolari indicate negli artt. 9 e 10 del Regolamento);

- controllerà le password in carico all'amministratore di sistema che dovranno avere una lunghezza minima di 8 caratteri e dovrà essere composta da almeno un numero, una lettera maiuscola, una minuscola e dove possibile un carattere speciale (per esempio: £, $, %, @, &, ecc.) e sostituite ogni sei mesi (3 mesi se i dati contenuti nei sistemi appartengono alle categorie particolari indicate negli artt. 9 e 10 del Regolamento);
- 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.

10. Informazione e formazione dei destinatari

L'obiettivo di garantire un corretto trattamento dei dati, conforme ai requisiti previsti dalla normativa[1], 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 comunica eventuali aggiornamenti con e-mail inviata a tutti i dipendenti. Questo regolamento viene inviato via email a tutti i dipendenti e affisso nella bacheca aziendale.

Allo scopo di formare i soggetti interni designati al trattamento, la Società:

1. adotta un piano formativo con l'obiettivo di alfabetizzazione in materia di protezione dei dati personali, destinato a tutto il personale della società;
2. 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;
3. prevede un piano di formazione programmato con cadenza annuale sulla formazione erogata in ambito della privacy a tutti i dipendenti della società;
4. 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 il personale sulle misure adeguate di sicurezza e protezione dei dati personali adottate dal titolare del trattamento;

[1] Art. 29 del GDPR - "Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento". Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

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., e può essere richiesta in qualsiasi momento da enti specifici.

11. 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 Regolamento 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 e all'autorità di controllo (allegato 2);
- il DPO terrà un registro dei data breach;
- il DPO, il soggetto interno designato o il responsabile esterno del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo 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.

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

- quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo;
- la comunicazione all'interessato descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere a), b), c) e d) del Regolamento;
- 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.

– Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni descritte al punto precedente sia soddisfatta.

13. Disposizioni interne per il corretto utilizzo degli strumenti informatici e telematici

La Società, con il seguente regolamento, si è dotata di procedure specifiche per l'uso dei sistemi informatici nonché l'accesso ad internet. Tali procedure, che vengono diffuse tra i dipendenti della Società con il seguente regolamento interno, hanno lo scopo di ridurre i rischi di natura patrimoniale, di danneggiamento di immagine della Società nonché di incorrere in responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge.
Le regole che disciplinano l'utilizzo delle risorse informatiche e telematiche si ispirano al principio della diligenza e correttezza, principi che normalmente si adottano nell'ambito dei rapporti di lavoro.
La mancata adozione delle misure indicate in questo regolamento da parte dei dipendenti espone gli stessi a provvedimenti disciplinari e risarcitori previsti dal vigente CCNL, nonché a tutte le azioni civili e penali consentite.

13.1. Utilizzo del personal computer e internet

Il Personal Computer affidato all'utente è uno strumento di lavoro, pertanto ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. È quindi assolutamente proibita la navigazione in Internet per motivi personali e diversi da quelli strettamente legati all'attività lavorativa.
Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.
L'amministratore di sistema, sotto indicazione titolare del trattamento e del DPO, ha la facoltà di collegarsi, in presenza dell'utente, alle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc.
Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dall'amministratore di sistema per conto della Società né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti.
L'inosservanza della presente disposizione espone la stessa Società a gravi responsabilità civili; si evidenzia, inoltre, che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate penalmente e possono anche comportare il sorgere di una responsabilità amministrativa a carico della società, come disposto dall'art. 25-novies del D.lgs. 8 giugno 2001, n. 231 e s.m.i., con applicazione di sanzioni pecuniarie ed interdittive.
Salvo autorizzazione dell'amministratore di sistema, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem ecc.).
Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'amministratore di rete nel caso in cui siano stati rilevati virus.
Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo, salvo disposizioni e/o richieste specifiche da parte dell'amministratore di sistema.
In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

Qualora, l'utente sia dotato di un PC portatile, egli è responsabile di custodirlo con diligenza sia se l'utilizzo avviene fuori sede sia durante l'utilizzo nel luogo di lavoro.
I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.
Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, la Società renderà peraltro nota l'adozione di uno specifico sistema di blocco o filtro automatico che previene determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una black list.
Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili nonché informazioni costituenti know-how aziendale, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.
I supporti magnetici contenenti dati relativi a persone fisiche devono essere adeguatamente custoditi dagli utenti in armadi chiusi. È vietato l'utilizzo di supporti rimovibili personali.
Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, ecc.) o per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, ecc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà del legale rappresentante, tramite l'amministratore di sistema, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.
Si mette a conoscenza tutti i lavoratori che la Sotacarbo è connessa alla rete telematica regionale (RTR) nei cui server sono contenuti i log di navigazione di ciascun ente collegato a tale sistema. Questi file log potranno essere visionati dai tecnici della Regione Autonoma della Sardegna senza nessun tipo di autorizzazione richiesta da parte della Regione a Sotacarbo.

13.2. Utilizzo dei PC portatili connessi al di fuori della rete aziendale

I dipendenti in missione che dovessero utilizzare dispositivi elettronici di proprietà della Sotacarbo e contenenti dati riferibili a persone fisiche, devono accertarsi che questi siano protetti da antivirus sempre aggiornati e che le reti wi-fi a cui si collegano siano sicure. I dati riconducibili a persone fisiche devono essere criptati e un eventuale data breach dovrà essere comunicato senza indugi al titolare del trattamento dati e al responsabile della protezione dati (DPO).

13.3. Utilizzo di dispositivi personali per lavoro

È fatto divieto a tutti i dipendenti l'utilizzo di propri dispositivi informatici per svolgere attività lavorativa per conto della Sotacarbo SpA.

13.4. Gestione sito web

13.4.1. Cookies policies

I cookies utilizzati sul Sito web aziendale hanno esclusivamente la finalità di eseguire autenticazioni informatiche o il monitoraggio di sessioni e la memorizzazione di informazioni tecniche specifiche riguardanti gli utenti che accedono ai server del titolare del trattamento che gestisce il Sito. In tale ottica, alcune operazioni sul Sito non potrebbero essere compiute senza l'uso dei cookies, che in tali casi sono quindi tecnicamente necessari. A titolo esemplificativo, l'accesso ad eventuali aree riservate del Sito e le attività che possono essere ivi svolte sarebbero molto più complesse da svolgere e meno sicure senza la presenza di cookies che consentono di identificare l'utente e mantenerne l'identificazione nell'ambito della sessione.
Il titolare del trattamento informa dunque che sul Sito sono operativi esclusivamente cookies tecnici (come quelli sopra elencati) necessari per navigare all'interno del Sito poiché consentono funzioni essenziali.
I cookies utilizzati per analizzare statisticamente gli accessi/le visite al sito (cookies cosiddetti "analytics") che perseguono esclusivamente scopi statistici (e non anche di profilazione o di marketing) e raccolgono

informazioni in forma aggregata senza possibilità di risalire alla identificazione del singolo utente. In questi casi, dal momento che la normativa vigente prescrive che per i cookies analytics sia fornita all'interessato l'indicazione chiara e adeguata delle modalità semplici per opporsi (opt-out) al loro impianto (compresi eventuali meccanismi di anonimizzazione dei cookies stessi), si specifica che è possibile procedere alla disattivazione dei cookies analytics come segue: aprire il proprio browser, selezionare il menu impostazioni, cliccare sulle opzioni internet, aprire la scheda relativa alla privacy e scegliere il desiderato livello di blocco cookies. Qualora si voglia eliminare i cookies già salvati in memoria è sufficiente aprire la scheda sicurezza ed eliminare la cronologia spuntando la casella "elimina cookies".

13.4.2. CV policies

Nel sito web aziendale è presente una sezione con le regole di trattamento dei dati dei curricola. Si rimenda ai punti 8.4 e 8.5 del seguente regolamento per le modalità di trattamento dei CV.

13.4.3. Social media policy

È fatto divieto a qualunque lavoratore di utilizzare i social media e i programmi di messaggistica istantanea relativamente ai dati riferibili a persona fisiche trattati per conto della Sotacarbo

13.5. Gestione email

Tutti i dipendenti dovranno prestare massima attenzione ai dati riferibili a persone fisiche che ricevono via mail, se configurabili come dati che permettono una profilazione della persona, devono dare immediata comunicazione al DPO che provvederà a fornire le opportune indicazioni. È fatto divieto inoltrare email dove sono presenti dati personali se non si dispongono delle necessarie autorizzazioni da parte della Società. I messaggi email contenenti dati personali devono avere un tempo di ritenzioni massima nel server aziendale di 12 mesi.
È vietato lo scambio di mail contenenti dati riferibili a persone fisiche utilizzando caselle di posta differenti da quelle Sotacarbo.it.

13.6. Gestione del Cloud aziendale

È fatto divieto a tutto il personale di caricare materiale coperto da copyright (musica, film, ebook, ecc.) nel proprio spazio assegnato dalla Società
A tutto il personale che è autorizzato a trattare dati personali particolari, di cui all'art.9 e art.10 del Regolamento, è fatto divieto di utilizzare il cloud per conservare questi dati, salvo casi eccezionali valutati insieme al DPO.
È consentito utilizzare questi spazi per tutti gli altri scopi connessi alla propria attività lavorativa.

13.7. Gestione delle credenziali di accesso

Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dall'amministratore di sistema previa formale richiesta del responsabile d'area nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente.
Nel caso di tirocinanti, stagisti e collaboratori esterni, la preventiva richiesta, se necessaria, verrà inoltrata direttamente dal responsabile dell'unità operativa con il quale il collaboratore si coordina nell'espletamento del proprio incarico.
Le credenziali di autenticazione per il personal computer consistono in un codice per l'identificazione dell'utente (user id) associato ad una password (vedasi punto 9.5 del presente regolamento) riservata che dovrà venir custodita dall'autorizzato con la massima diligenza e non divulgata. Le credenziali di autenticazione per il sistema HR consistono in una user id, una password ed un codice identificativo.
Le credenziali di accesso alla rete wi-fi aziendale sono riservate ai soli dipendenti (tempo determinato e indeterminato) della Sotacarbo e non possono essere cedute a terzi.

13.8. Centro Ricerche

Le porte di accesso al centro ricerche Sotacarbo devono sempre rimane chiuse. Ad ogni dipendente viene consegnato il codice numerico di accesso al centro ricerche da parte del responsabile della gestione del centro, che dovrà essere conservata con cura e non diffusa a persone terze. Gli ospiti potranno accedere al Centro utilizzando l'apposito citofono.

14. Gestione dei dati dei dipendenti e degli ospiti del Centro Ricerche

14.1. Dipendenti

14.1.1. Dati medici dei dipendenti

I referti delle analisi mediche effettuate dal medico competente devono essere inviati solamente alle email che la società ha attivato per ogni dipendente. È consentito la consegna a mano al lavoratore, solamente in busta chiusa e direttamente dal medico competente o da persona da lui incaricata.

14.1.2. Gestione dei certificati di malattia e di visita medica

I certificati di malattia o di visita medica devono essere consegnati a mano o tramite email solamente al consulente del lavoro, nominato responsabile esterno del trattamento. Il dipendente comunicherà, via email, al proprio superiore gerarchico e in copia all'incaricato/a revisione delle timbrature solamente il periodo di assenza, senza indicare nessun'altra informazione (p.e. il numero di protocollo dell'INPS).

14.1.3. Gestione delle buste paga

Le buste paga devono essere consegnate ai dipendenti secondo le seguenti modalità nel rispetto della privacy:

- in busta chiusa direttamente al lavoratore e non tramite intermediari;
- tramite la casella di posta elettronica, sia certificata che non, che la Società ha attivato per ogni dipendente.

14.1.4. Videosorveglianza

Il sistema di video sorveglianza e il trattamento dei dati con esso acquisiti sono gestiti da apposito accordo sindacale e ordine di servizio interno

14.2. Ospiti

14.2.1. Accesso al Centro Ricerche e all'area degli impianti sperimentali

Per gli ospiti si adotta la seguente procedura:
Il visitatore e/o lavoratore di una ditta terza, dovrà accedere esclusivamente dall'ingresso principale passando per la portineria, il cui addetto/a provvederà a consegnare la brochure e il modulo di dichiarazione di presa visione del documento, con inclusa l'informativa privacy, che dovrà essere compilato e firmato. Il visitatore sarà sempre accompagnato da un dipendente della Sotacarbo all'interno del Centro Ricerche e degli impianti sperimentali. Ad ogni ospite verrà consegnato un badge che deve essere sempre visibile per una immediata identificazione della persona. Nel caso delle ditte terze il badge NON sostituisce il cartellino obbligatorio, contenente i dati identificativi della ditta e del lavoratore. Nel caso in cui non fosse presente il personale di portineria, la suddetta procedura dovrà essere eseguita direttamente dall'accompagnatore Sotacarbo.

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.

Carbonia, 4 novembre 2019

Allegato 1

Organigramma Privacy

Titolare del trattamento:	Sotacarbo SpA
Data Protection Officer (DPO):	ing. Enrico Maggio;
Amministratore di sistema:	ing. Fabrizio Tedde;

Designati interni al trattamento

- Responsabile amministrazione:	dott. Andrea Barbarossa
- Responsabile protocollo e RUP:	rag. Massimiliano Demurtas
- Responsabile rendicontazione progetti:	ing. Marcella Fadda
- Responsabile scientifico:	ing. Alberto Pettinau
- Rappresentante dei lavoratori per la sicurezza:	ing. Andrea Porcu
- Responsabile ufficio bandi e gare:	dott.ssa Anna Maria Puggioni
- Responsabile trasparenza e comunicazione:	dott. Gianni Serra
- Responsabile officina meccanica:	sig. Antonio Argiolas
- Responsabile Unita operativa:	ing. Gabriele Calì
- Responsabile Unico del procedimento (RUP):	dott. Rafaele Cara
- Responsabile Unita operativa:	ing. Francesca Ferrara
- Responsabile Unita operativa:	ing. Caterina Frau
- Responsabile Unico del procedimento (RUP):	ing. Diana Multineddu
- Responsabile Unita operativa:	dott. Alberto Plaisant
- incaricato rendicontazione progetti:	dott. Giovanni Perra;
- Responsabile Unita operativa:	ing. Alessandro Orsini
- Responsabile Unico del procedimento (RUP):	ing. Fabrizio Tedde
- Incaricata revisione timbrature	rag. Romina Moi

Responsabili esterni

- Dott. Luca Camporelli	Consulente del lavoro
- Ing. Claudio Cristofori della IT Technologies	Programma gestione Human Resources
- Sig. Gianluca Serra	Responsabile Servizio Prevenzione e protezione
- Avv. Marcello Spissu	Organismo di vigilanza

Titolare Autonomo

- Dott.ssa Giulia Gigli	Medico competente

SOTACARBO
SUSTAINABLE ENERGY RESEARCH CENTRE

Allegato 2

MODELLO DI COMUNICAZIONE DI DATA BREACH AL GARANTE

Denominazione o ragione sociale: Sotacarbo SpA
Provincia Sud Sardegna **Comune** Carbonia
Cap 09016 **Indirizzo** Grande Miniera Serbariu snc
Nome persona fisica addetta alla comunicazione
Cognome persona fisica addetta alla comunicazione
Funzione rivestita
Indirizzo Email per eventuali comunicazioni
Recapito telefonico per eventuali comunicazioni
Titolare che effettua la comunicazione
Eventuali Contatti (altre informazioni)
Natura della comunicazione

- ☐ Nuova Comunicazione
- ☐ Modifica di una comunicazione esistente
- ☐ Ritiro di una comunicazione

Breve descrizione della violazione di dati personali

Quando si è verificata la violazione di dati personali?

- ☐ Il _____
- ☐ Tra il _____e il _____
- ☐ In un tempo non ancora determinato
- ☐ E' possibile che sia ancora in corso

Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di dispositivi o di supporti portatili)

Modalità di esposizione al rischio?

Tipo di violazione

- ☐ Lettura (presumibilmente i dati non sono stati copiati)
- ☐ Copia (i dati sono ancora presenti sui sistemi del titolare)
- ☐ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
- ☐ Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
- ☐ Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)
- ☐ Altro :

Dispositivo oggetto della violazione

- ☐ Computer
- ☐ Dispositivo mobile
- ☐ Documento cartaceo

☐ File o parte di un file
☐ Strumento di backup
☐ Rete
☐ Altro :

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione:

Quante persone sono state colpite dalla violazione di dati personali?
☐ N. _____di persone
☐ Circa_____ persone
☐ Un numero (ancora) sconosciuto di persone

Che tipo di dati sono coinvolti nella violazione?
☐ Dati anagrafici
☐ Numero di telefono (fisso o mobile)
☐ Indirizzo di posta elettronica
☐ Dati di accesso e di identificazione (user name, password, customer ID, altro)
☐ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro)
☐ Altri dati di personali (sesso, data di nascità, età, ...), dati sensibili e giudiziari
☐ Ancora sconosciuto
☐ Altro :

Livello di gravità della violazione dei dati personali (secondo le valutazioni del titolare)?
☐ Basso/trascurabile
☐ Medio
☐ Alto
☐ Molto alto

Misure tecniche e organizzative applicate ai dati colpiti dalla violazione

La violazione è stata comunicata anche a contraenti (o ad altre persone interessate)?
☐ Sì, è stata comunicata il _____
☐ No, perchè

Qual è il contenuto della comunicazione ai contraenti (o alle persone interessate)?

Quale canale è utilizzato per la comunicazione ai contraenti (o alle altre persone interessate)?

Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?

La violazione coinvolge contraenti (o altre persone interessate) che si trovano in altri Paesi UE?

☐ Sì
☐ No

La comunicazione è stata effettuata alle competenti autorità di altri Paesi UE?

☐ No
☐ Sì