SeaCorridor

GUIDELINE

PRIVACY E DATA PROTECTION

Data	Rev.	Process Owner	Verifica	Approvazione
20/03/2023	0	Valentina Milazzo	Luigi A. Ferrario	Francesco Caria

Tracking revisioni		
Revisione	**Data rilascio**	**Modifiche rilevanti**
0	20/03/2023	Primo rilascio

Sommario

1. Introduzione

1.1. Obiettivi del documento

Obiettivo della presente Guideline è definire un sistema di compliance Privacy e di regole atti a garantire che il Trattamento dei Dati Personali sia effettuato in modo conforme alle normative applicabili e nel rispetto dei diritti dell'Interessato.

In essa sono disciplinati i ruoli e le responsabilità, nonché gli adempimenti da seguire in materia di protezione dei Dati Personali ai sensi della normativa applicabile.

1.2. Ambito di applicazione

La presente Guideline si applica a:

- SeaCorridor Srl;
- Società Controllate di SeaCorridor Srl, direttamente e indirettamente, in Italia e all'estero, previo recepimento secondo le modalità descritte nel successivo capitolo 1.3 e dal successivo capitolo 5.

Le Società partecipate valutano in autonomia l'eventuale recepimento, sempre secondo le modalità descritte nel capitolo 1.3.

1.3. Modalità di recepimento

La presente Guideline è di applicazione immediata per SeaCorridor.

Le Società Controllate aventi sede nel territorio comunitario assicurano il recepimento tempestivo della presente Guideline, secondo le modalità descritte nella Guideline "Sistema Normativo" di SeaCorridor.

Le Società Controllate aventi sede fuori dal territorio comunitario assicurano il recepimento tempestivo, per quanto compatibile, della presente Guideline, in ogni caso nei limiti di quanto indicato nel capitolo 5 secondo le modalità descritte nella Guideline "Sistema Normativo" di SeaCorridor.

Per le società non sottoposte a controllo SeaCorridor, il board di nomina SeaCorridor si adopererà, al meglio delle sue possibilità, per garantire il massimo recepimento possibile della presente Guideline dalla società partecipata.

2. Principi di riferimento

Si riportano di seguito i principi di riferimento della disciplina normativa in materia di Privacy e Data Protection:

RESPONSABILIZZAZIONE: Tutte le Persone di SeaCorridor a vario titolo coinvolte nella conduzione degli affari di SeaCorridor, che svolgono attività di Trattamento dei Dati Personali, devono garantire il rispetto dei presenti principi di riferimento, la corretta applicazione della Guideline e, più in generale, delle disposizioni applicabili in tema di Trattamento dei Dati Personali.

APPROCCIO RISK BASED: SeaCorridor adotta un approccio "risk-based" nella definizione delle azioni di mitigazione da porre in essere rispetto al rischio di non conformità, prevedendo azioni di mitigazione e attività di monitoraggio e reporting proporzionate rispetto al livello di rischio associabile all'attività oggetto del controllo.

CORRETTEZZA E TRASPARENZA: I Dati Personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'Interessato. Il Trattamento deve sempre essere giustificato da una valida Base Giuridica.

PERTINENZA E NECESSITÀ: I Dati Personali sono raccolti per finalità determinate, esplicite e legittime, sono pertinenti e limitati a quanto strettamente necessario rispetto alle finalità per le quali sono raccolti e vengono successivamente trattati in modi non incompatibili con tali finalità. Il Trattamento deve rientrare nelle finalità per cui l'Interessato ha conferito i Dati Personali e/o il proprio consenso, espressamente indicate nell'Informativa.

ESATTEZZA: I Dati Personali devono essere esatti e, se necessario, aggiornati. Devono essere adottate tutte le misure ragionevoli per cancellare/rettificare tempestivamente i Dati inesatti.

CONSERVAZIONE: I Dati Personali devono essere conservati in una forma che consenta l'identificazione degli Interessati per un tempo non superiore al conseguimento delle finalità per cui sono trattati. Una volta che vengono meno le finalità per cui i Dati Personali sono stati raccolti, gli stessi devono essere distrutti o de-identificati.

INTEGRITÀ E SICUREZZA: I Dati Personali devono essere trattati in modo da garantire un'adeguata sicurezza degli stessi, compresa la protezione da trattamenti illeciti o non autorizzati e da perdita, distruzione, danni accidentali. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del Trattamento, come anche del rischio per i diritti e le libertà degli Interessati, sono adottate misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio, secondo la best practice del settore e in conformità, qualora richiesta, con la Valutazione di Impatto rispetto ai singoli Trattamenti. Ogni volta che sono effettuate operazioni di Trattamento dei Dati Personali, occorre adottare l'attenzione e la prudenza dovute.

TUTELA DEI DIRITTI DELL'INTERESSATO: SeaCorridor Srl e ciascuna delle Società Controllate, in qualità di Titolari del Trattamento dei Dati Personali, adottano le misure appropriate per fornire all'Interessato tutte le informazioni relative al Trattamento dei suoi Dati Personali, nonché per tutelare i Diritti dell'Interessato, fermi restando i limiti previsti dalla legge e da altri strumenti normativi applicabili in materia. È necessario, da parte delle competenti funzioni, prendere in carico senza indugio le legittime

richieste formulate dagli Interessati (es. clienti, dipendenti, terze parti) rispetto al Trattamento dei Dati Personali dell'Interessato.

Le risposte all'Interessato devono essere fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici in forma concisa, trasparente e con un linguaggio semplice e chiaro.

3. Definizioni, abbreviazioni ed acronimi

AMMINISTRATORE DI SISTEMA: figura professionale[1] che mantiene, configura e gestisce

- un sistema di elaborazione dati o sue componenti, ivi inclusi sistemi software complessi quali i sistemi Enterprise Resource Planning (system administrator),
- una base dati (database administrator),
- reti e apparati di telecomunicazione di sicurezza (*network administrator*).

AUTORITÀ DI CONTROLLO: l'autorità pubblica indipendente, prevista dal GDPR, istituita da uno Stato Membro[2] al fine di sorvegliare l'applicazione della normativa in materia di protezione dei Dati Personali.

BASE GIURIDICA: è il fondamento giuridico necessario a giustificare il Trattamento. Le basi giuridiche che rendono lecito il Trattamento sono quelle previste dagli articoli 6 e 9 del Regolamento (UE) 2016/679.

CONSENSO: 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, sul Trattamento dei Dati Personali che lo riguardano in relazione ad una specifica attività.

DATA RECORD OWNER: ruolo aziendale cui, ai sensi della presente Guideline, sono affidate le responsabilità previste al Capitolo 6.

DATO PERSONALE (O ANCHE DATO): nella presente Guideline qualunque informazione riguardante una persona fisica identificata o identificabile. 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 personale (es. codice identificativo dipendente), un codice identificativo online, Dati relativi all'ubicazione[3], un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. Con riferimento alla natura del dato trattato i Dati Personali si distinguono in diverse categorie, quali:

- *Dati Sensibili:* Dati Personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, la vita sessuale o l'orientamento sessuale della persona, nonché Dati genetici;
- *Dati Biometrici:* Dati Personali ottenuti da un Trattamento 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;

[1] Prevista dalla normativa italiana in ambito informatico.
[2] I riferimenti agli "Stati membri" vanno intesi come riferimenti agli "Stati membri dello Spazio Economico Europeo (di seguito, SEE)".
[3] Inclusi i dati che forniscono l'indicazione della posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica (geolocalizzazione).

- Dati relativi alla salute: Dati Personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- Dati Giudiziari: Dati Personali idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 del Codice di Procedura Penale.

DELEGATO DEL TITOLARE: la persona fisica che, nell'ambito dell'organizzazione societaria, esercita le funzioni (diritti, facoltà ed obblighi) riservate dalla legge al Titolare del Trattamento ed individuato in SeaCorridor Srl e in ciascuna delle Società Controllate secondo quanto previsto al successivo Capitolo 6.

DIRITTI DELL'INTERESSATO: sono i diritti riconosciuti all'Interessato in relazione alla conoscenza e trasparenza dei Trattamenti di Dati Personali che lo riguardano, rispetto al diritto di accesso ai propri Dati Personali, al diritto di integrazione e di rettifica, al diritto alla cancellazione dei Dati Personali e al diritto all'oblio[4], al diritto alla portabilità dei Dati Personali e al diritto alla limitazione, seppur per brevi periodi, del Trattamento.

SEACORRIDOR: SeaCorridor Srl e, ove non diversamente precisato, le sue Società Controllate direttamente e indirettamente in Italia e all'estero.

FINALITÀ DEL TRATTAMENTO: scopo perseguito dal Titolare del Trattamento per specifiche operazioni di Trattamento dei Dati Personali.

GARANTE DELLA PRIVACY (O ANCHE GARANTE): il Garante per la protezione dei Dati Personali, ossia l'Autorità di Controllo istituita nel territorio italiano, ai sensi della normativa italiana.

GDPR: Regolamento UE n. 2016/679 "Regolamento Generale sulla protezione dei Dati", unitamente ai relativi atti d'implementazione e loro successive modifiche o integrazioni.

INFORMATIVA: insieme di informazioni fornite all'Interessato dal Titolare del Trattamento circa il Trattamento posto in essere da quest'ultimo.

INTERESSATO: la persona fisica, prevista dalle normative italiane ed europee, cui si riferiscono i Dati Personali.

ISTRUZIONI: l'insieme delle direttive, regole, informazioni scritte relative a mansioni, attività e compiti per le quali è necessario fornire alle Persone di SeaCorridor idonea spiegazione circa le caratteristiche e le modalità di esecuzione delle stesse. Esse sono composte da una parte generale (Istruzioni generali), definita dal Delegato del Titolare, e una parte eventuale, specifica (Istruzioni specifiche), predisposta dal Data Record Owner.

[4] Inteso come l'interesse di un singolo ad essere dimenticato; l'esercizio di tale diritto consiste nella cancellazione dei contenuti, dalle varie pagine web, di precedenti informazioni (spesso pregiudizievoli come, ad esempio, precedenti penali) che non rappresentano più la vera identità dello stesso interessato.

PERSONA AUTORIZZATA[5] AL TRATTAMENTO: la persona fisica, prevista dalle normative italiane ed europee[6], che, nell'adempimento delle proprie mansioni, compie operazioni di Trattamento, secondo quanto previsto al successivo Capitolo 6.

PERSONE DI SEACORRIDOR: ai fini della presente Guideline si intendono i membri degli organi di amministrazione, di controllo/di vigilanza, il management nonché i dipendenti e i collaboratori[7], individuati come Persone Autorizzate al Trattamento dei Dati Personali e destinatari pertanto delle Istruzioni.

PRIVACY BY DESIGN E PRIVACY BY DEFAULT: si intende il complesso di misure tecniche e organizzative volte ad attuare in modo efficace i principi di protezione dei Dati Personali, quali la minimizzazione, la pseudonimizzazione, etc. nonché ulteriori garanzie al fine di tutelare i diritti degli Interessati tanto nei prodotti che nei servizi offerti da SeaCorridor e da ciascuna delle Società Controllate, quanto più in generale, rispetto alle modalità di esecuzione delle operazioni di Trattamento dei Dati Personali.

PRIVACY E DATA PROTECTION (O ANCHE "PRIVACY"): è il diritto alla protezione dei Dati di carattere personale che riguardano l'interessato nell'ambito dei trattamenti effettuati da SeaCorridor in relazione ai rapporti contrattuali con la stessa.

PROCESS OWNER: è il Process Owner previsto dalla Guideline "Sistema Normativo" di SeaCorridor; ai sensi della presente Guideline, è responsabile dell'adeguatezza del disegno dei processi e delle relative Guideline, per quanto riguarda il Trattamento dei Dati Personali in conformità alla presente Guideline e agli obblighi previsti dal GDPR, nonché del rispetto delle relative regole di compliance o governance di propria competenza.

RECLAMO: ai fini della presente Guideline si intende ogni comunicazione e/o richiesta, trasmissione di notizie fatta con qualsiasi mezzo da parte dell'Interessato al Titolare o all'Autorità di Controllo in relazione ai fatti e alle circostanze che potrebbero determinare o che hanno determinato una violazione delle disposizioni in materia di protezione Dati Personali.

REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO (O REGISTRO): il documento, anche informatico, che ogni Data Record Owner per l'area per cui è stato individuato, deve compilare e mantenere aggiornato, contenente:

- indicazione delle finalità del Trattamento,
- elenco delle categorie di Dati e di Interessati,
- indicazione dei destinatari e dei trasferimenti,
- le misure di sicurezza adottate,

[5] Il concetto di autorizzazione non è legato ad un atto formale di nomina/autorizzazione specifica.
[6] L'art. 4, n. 10 del GDPR fa riferimento a persone autorizzate al trattamento dei dati sotto l'autorità diretta del titolare o del responsabile.
[7] Ai fini della presente Guideline, si intendono i collaboratori coordinati e continuativi.

- l'elenco dei responsabili del Trattamento esterni. Congiuntamente considerati, tali Registri andranno a costituire il Registro delle attività di Trattamento di SeaCorridor (o Registro Consolidato) o di ciascuna delle Società Controllate.

RESPONSABILE PER LA PROTEZIONE DEI DATI PERSONALI (O ANCHE "DATA PROTECTION OFFICER" O ANCHE "DPO"): organismo aziendale, previsto dal GDPR, cui sono affidate le funzioni di cui al Capitolo 6.

SOCIETÀ CONTROLLATE: società direttamente e/o indirettamente controllate, in via solitaria[8], da SeaCorridor Srl, in Italia e all'estero, elencate nell'allegato "Imprese controllate" dell'ultimo bilancio consolidato approvato, nonché nell'elenco integrativo relativo alle società italiane controllate di diritto, ai sensi dell'art. 2359, comma 1, n. 1, e comma 2, del codice civile, da SeaCorridor, predisposto dalla funzione "LEGAL AND COMPLIANCE" sentita la competente unità della funzione "PLANNING & CONTROL, ADMINISTRATION AND FINANCE", nonché le altre funzioni competenti individuate con il supporto della Funzione "HR AND SERVICES", e messo a disposizione delle funzioni interessate per gli adempimenti previsti dalla applicabile.

TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI (O ANCHE TITOLARE): persona fisica o giuridica che, singolarmente o insieme ad altri, determina le finalità e i mezzi del Trattamento. Titolare del Trattamento sono pertanto SeaCorridor e ciascuna delle Società Controllate che rientrano nell'ambito d'applicazione della presente Guideline;

TRASFERIMENTO: trasferimento di Dati Personali verso un Paese extra-UE o un'organizzazione internazionale;

TRATTAMENTO DEI DATI PERSONALI (O ANCHE TRATTAMENTO): qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati ed 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;

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (O ANCHE "DATA PROTECTION IMPACT ASSESSMENT" O "DPIA"): valutazione dell'impatto e dei rischi per i diritti e le libertà delle persone fisiche relativi ai Trattamenti di Dati Personali effettuati da SeaCorridor in ragione delle tecnologie utilizzate e considerati la natura, l'oggetto, il contesto e le finalità dei singoli trattamenti;

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.

[8] Per Società direttamente e/o indirettamente Controllate in via solitaria da SeaCorridor si intendono le società in cui SeaCorridor esercita un controllo, diretto e/o indiretto, anche non necessariamente attraverso una partecipazione totalitaria, non condiviso con Soci terzi.

4. Identificazione delle funzioni di supporto[9]

FUNZIONE HR COMPETENTE: si intende la funzione "HR AND SERVICES" di SeaCorridor e delle Società Controllate, responsabile:

- della gestione del personale di competenza
- delle attività relative al processo ICT;
- delle funzioni ICT, ove presenti, delle Società Controllate; ai fini della presente Guideline, ha la responsabilità - per i sistemi gestiti – di:
  - supportare il Data Record Owner nella definizione delle misure di sicurezza nell'ambito della Valutazione di Impatto sulla protezione dei Dati;
  - supportare l'Unità Compliance Privacy in caso di denuncia di Violazione dei Dati Personali;
  - designare gli Amministratori di Sistema;
- responsabile dell'adozione delle misure di sicurezza nell'ambito delle proprie funzioni.

FUNZIONE "LEGAL AND COMPLIANCE": si intende l'unità organizzativa competente in materia di privacy e protezione dei dati personali[10], di cui al capitolo 6 e in materia di *risk assessment* (e di supporto in materia di DPIA) e in materia di compliance monitoring.

[9] Ogni richiamo a strutture od unità organizzative contenuto nella presente Guideline deve intendersi effettuato anche con riferimento alle strutture od unità organizzative, diversamente denominate che, in virtù di disposizioni organizzative intervenute successivamente all'emissione della presente Guideline, dovessero sostituire le prime in tutto o in via prevalente.
[10] Laddove le Società Controllate, per la natura delle loro attività e per la quantità di dati personali trattati, si siano dotate di un presidio specialistico in materia di privacy, le attività di consulenza e di assistenza alla società (incluse le attività di supporto agli adempimenti di compliance) sono garantite da tale presidio specialistico al fine dell'efficace ed efficiente adozione dei modelli di compliance, promuovendo un approccio di compliance by design.

5. Modalità di applicazione

5.1. Ambito di applicazione materiale

Oggetto della presente Guideline è il Trattamento, automatizzato e non, di Dati Personali contenuti o destinati a figurare in un archivio cartaceo o informatico.

Sono esclusi dall'ambito di applicazione i Trattamenti dei Dati Personali effettuati da persone fisiche per fini esclusivamente personali[11] e nei casi in cui tali dati non siano destinati ad una comunicazione sistematica o alla diffusione, anche se utilizzati ai fini di esigenze di lavoro (ad esempio, banca dati su personal computer accessibile ed utilizzata solo ed esclusivamente dall'utente/persona fisica, rubrica telefonica, foto personali, esiti di esami clinici/diagnostici, ecc.).

5.2. Ambito di applicazione territoriale

Le norme della presente Guideline si applicano al Trattamento di Dati Personali effettuato da:

- SeaCorridor[12], indipendentemente dal fatto che lo stesso sia effettuato o meno nell'Unione Europea;
- le Società Controllate stabilite nell' Unione Europea, indipendentemente dal fatto che lo stesso sia effettuato o meno nell' Unione Europea;
- le Società Controllate stabilite al di fuori dell'Unione Europea nell'ambito delle attività di uno stabilimento[13] situato all'interno dell'Unione Europea, indipendentemente dal fatto che il Trattamento dei Dati Personali venga svolto o meno nell'Unione Europea.

Le Società Controllate stabilite nell'Unione Europea recepiscono la presente Guideline, ai sensi del paragrafo 1.3.

Le branches di Società Controllate UE, stabilite in Paesi extra comunitari, che effettuano Trattamenti dei Dati Personali fuori dall'Unione Europea, si adeguano ai principi di riferimento di cui al capitolo 2, che costituiscono le linee guida di indirizzo generale per il Trattamento dei Dati Personali.

Inoltre, le Società Controllate stabilite nell'Unione Europea, a seguito del recepimento della presente Guideline, adottano, con il supporto della funzione Organizzazione competente, eventuali strumenti normativi di dettaglio in ottemperanza alle normative locali o a provvedimenti emessi dall'Autorità di Controllo del Paese di appartenenza. L'adozione di tali eventuali strumenti normativi è condivisa con l'Unità Compliance Privacy.

Le Società Controllate stabilite al di fuori dell'Unione Europea recepiscono la presente Guideline, ai sensi del paragrafo 1.3, per utilizzarne i contenuti ai fini di:

[11] Tali Dati devono essere facilmente individuabili, ad esempio all'interno di cartelle appositamente denominate con la dicitura "personale".
[12] Sia in qualità di Titolare, sia in quella di Responsabile del Trattamento.
[13] Per "Stabilimento" si intende qualsiasi attività reale ed effettiva, anche minima, esercitata tramite un'organizzazione stabile nell'UE, a prescindere dalla forma giuridica assunta (Corte di giustizia dell'UE nei casi Weltimmo vs NAIH e Google Spain SL, Google Inc. V AEPD, Mario Costeja Gonzàlez).

- adottare i principi di riferimento di cui al capitolo 2, come linea guida generale per il Trattamento dei Dati Personali;
- applicarne interamente i contenuti in relazione, ove esistenti, ai Trattamenti di Dati Personali:
    - concernenti l'offerta di beni o la prestazione di servizi (es. vendita di prodotti/servizi) agli Interessati nell'Unione Europea[14]; e/o
    - che comprendono il monitoraggio (es. profilazione) del comportamento di Interessati che ha luogo nell'Unione Europea (es. profilazione dei consumatori europei relativa alle abitudini di consumo desunte dal comportamento degli stessi consumatori su una piattaforma di commercio on-line gestita dalla società di cui trattasi[15]).

Le Società Controllate stabilite fuori dall'Unione Europea adottano eventuali strumenti normativi di dettaglio in ottemperanza alle normative locali o a provvedimenti emessi dall'Autorità di Controllo del Paese di appartenenza.

L'adozione di tali eventuali strumenti normativi è condivisa con la funzione "LEGAL AND COMPLIANCE".

[14] Ad esempio, dati trattati da aziende di commercio elettronico attraverso piattaforme di vendite online.
[15] Ad esempio, dati trattati attraverso social network.

6. Ruoli e responsabilità nel modello di compliance privacy

Nel presente Capitolo sono declinati i ruoli e le principali responsabilità delle figure aziendali coinvolte nell'applicazione del modello di compliance Privacy definito nella presente Guideline, nell'ottica di collocarli all'interno delle posizioni organizzative che operativamente siano più idonee a mettere in atto le azioni e a garantire gli adempimenti ad esso sottesi.

Nel caso di ruoli per cui è prevista una nomina formale si fa riferimento agli standard di nomina resi disponibili nel sistema in cui vengono pubblicati gli strumenti normativi.

Le funzioni della Società SeaCorridor e di ciascuna delle Società Controllate riceveranno supporto dalle funzioni di competenza delle Società Controllanti in coerenza con i Contratti di Servizio volta per volta in essere.

6.1. Titolare del Trattamento dei Dati Personali

Il Titolare del Trattamento dei Dati Personali è individuato nella persona giuridica di SeaCorridor e di ciascuna delle Società Controllate che rientrano nell'ambito d'applicazione della presente Guideline. La singola Società Controllata può individuare un Delegato del Titolare, che esercita i compiti definiti nel successivo paragrafo 6.2.

6.2. Delegato del Titolare

In SeaCorridor il Delegato del Titolare è individuato nel Responsabile della funzione "LEGAL AND COMPLIANCE".

Nelle Società Controllate in ambito UE, il ruolo di Delegato del Titolare è svolto, di norma, dall'Amministratore Unico o dall'Amministratore Delegato/*Managing Director*[16] (o figura equivalente) individuato con delibera del Consiglio di Amministrazione/*Board of Director* di ciascuna Società Controllata.

Il Delegato del Titolare, munito dei necessari poteri, ha la responsabilità di:

- coordinare il sistema di compliance Privacy nel suo complesso, assicurandone l'efficacia e l'efficienza;
- designare i Responsabili del Trattamento esterni[17] (o delegare altri procuratori alla loro nomina) e i Data Record Owner, questi ultimi, sentita la funzione "HR AND SERVICES" e il Process Owner;
- nominare e revocare[18] il DPO;
- rappresentare la società in relazione a tutte le questioni relative alla tutela dei Dati Personali innanzi all'Autorità di Controllo, nominando eventualmente procuratori speciali e consulenti;
- definire il disegno per l'esecuzione del Data Protection Impact Assessment (DPIA) tramite i ruoli individuati dalla presente Guideline;

[16] Compreso, per le società in liquidazione, il Liquidatore (o figura equivalente in caso di società estere).
[17] Per i Responsabili del Trattamento esterni si veda paragrafo 6.10.
[18] La nomina del DPO da parte delle Società Controllate avviene nell'ambito della delibera di adozione della presente Guideline.

- individua, ad esito delle attività di risk assessment, i criteri per l'adozione delle misure di sicurezza;
- impartire le regole di indirizzo ai Data Record Owner, al momento della designazione;
- impartire le Istruzioni generali che le Persone Autorizzate al Trattamento devono seguire per assicurare che i Trattamenti avvengano in coerenza a tutto quanto previsto dalla normativa applicabile e nella presente Guideline.

Il Delegato del Titolare svolge le proprie funzioni per il tramite del DPO (Data Protection Officer), della funzione "LEGAL AND COMPLIANCE", della funzione "HR AND SERVICES", nonché dei Process Owner e dei Data Record Owner, ciascuno in relazione agli ambiti di rispettiva competenza.

Le misure organizzative per garantire la concreta attuazione del modello di compliance privacy sono implementate dalle figure aziendali responsabili delle attività cui inerisce il Trattamento dei Dati Personali.

6.3. Process Owner

In coerenza con quanto disciplinato dalla Guideline "Sistema Normativo" di SeaCorridor, ciascun Process Owner garantisce, col supporto, ove richiesto, della funzione "LEGAL AND COMPLIANCE", che nel disegno dei processi e delle relative Guideline di propria competenza i Dati Personali vengano trattati in conformità alla presente Guideline, agli obblighi previsti dal GDPR tenendo conto della natura dei Dati Personali trattati nel processo presidiato.

Inoltre, il Process Owner segnala tempestivamente al DPO, anche per il tramite dei Data Record Owner, qualsiasi possibile Violazione di Dati Personali (anche solo sospetta) di cui direttamente e/o indirettamente venga a conoscenza.

Infine, il Process Owner si coordina con l'Unità "LEGAL AND COMPLIANCE" e con il Data Record Owner di riferimento per la verifica di eventuali impatti di tematiche relative alla privacy e data protection sugli strumenti normativi di propria competenza.

6.4. Data Record Owner

In funzione della complessità organizzativa, in SeaCorridor e nelle Società Controllate, sono individuati i Data Record Owner, seguendo criteri di efficienza, semplificazione e vista trasversale dei processi.

Tale ruolo può essere adeguatamente svolto sia da una struttura alle dipendenze del Process Owner nell'ambito del processo di propria competenza, sia dalle funzioni di Compliance Business Support, ove presenti nei business.

Ciascun Data Record Owner, con il supporto della funzione "LEGAL AND COMPLIANCE" e, ove necessario, della funzione "HR AND SERVICES", ha per gli ambiti per i quali è nominato i seguenti compiti:

- fornisce supporto affinché vengano effettuati tutti gli adempimenti su tutti gli aspetti relativi al sistema di gestione della compliance privacy di ciascun Trattamento quali, a titolo esemplificativo e non esaustivo:
  i. Informativa agli Interessati;
  ii. Istruzioni alle Persone Autorizzate al Trattamento;

iii. svolgimento -quando e se necessario- del bilanciamento di interessi (LIA);
iv. svolgimento -quando e se necessario- della Valutazione d'Impatto, etc.;

- è cura della funzione "LEGAL AND COMPLIANCE" segnalare al Data Record Owner gli ulteriori adempimenti che si renderanno necessari a fronte di modifiche nella normativa;
- effettua il corretto censimento delle categorie di operazioni di Trattamento Dati Personali, che sono eseguiti nell'area di competenza nonché degli archivi cartacei e dei database utilizzati per le attività di Trattamento;
- assicura la compilazione e l'aggiornamento del Registro delle Attività di Trattamento per cui è stato individuato;
- supporta, in coordinamento con la funzione "LEGAL AND COMPLIANCE", la funzione "HR AND SERVICES" nella valutazione e successiva adozione delle misure minime di sicurezza secondo quanto previsto dal GDPR e dalle normative aziendali applicabili in materia di sicurezza, e nei relativi aggiornamenti;
- contribuisce al processo di monitoraggio della corretta implementazione della presente Guideline, in particolare attraverso la compilazione della lettera di attestazione annuale di cui al paragrafo 7.6.1;
- fornisce supporto alla funzione "LEGAL AND COMPLIANCE" in caso di richieste di informazioni e nello svolgimento dei controlli e degli accessi da parte delle Autorità competenti per la protezione dei Dati Personali e di altre Autorità pubbliche competenti nonché in caso di verifiche e controlli interni, in materia di Privacy e Data Protection;
- fornisce all'Unità Compliance Privacy ogni supporto utile a individuare i fabbisogni formativi e promuovere e realizzare piani di formazione in materia di privacy e data protection;
- garantisce che il Trattamento dei Dati Personali effettuati all'interno della propria struttura e la tenuta dei relativi archivi cartacei e informatici siano conformi a quanto previsto nella presente Guideline e che siano adottate e rispettate le misure tecniche e organizzative individuate dalla funzione "HR AND SERVICES" in coerenza con gli standard di sicurezza adottati dall'azienda;
- fornisce le indicazioni e si adopera affinché le azioni previste dal presente strumento normativo siano poste in essere dai propri collaboratori o consulenti, che nell'ambito dell'attività lavorativa compiano operazioni di Trattamento di Dati Personali, affinché rispettino le istruzioni ricevute con particolare riguardo all'accesso ai sistemi in uso e al rispetto delle suddette misure di sicurezza;
- informa senza indugio il Process Owner e il DPO di eventuali violazioni dei Dati, sospettate o effettive, che si siano verificate nell'ambito delle attività di Trattamento dei Dati Personali nella struttura di competenza;
- fornisce collaborazione alla funzione "LEGAL AND COMPLIANCE" in caso di richieste di informazioni e nello svolgimento dei controlli e degli accessi da parte delle Autorità competenti per la protezione dei Dati Personali e di altre Autorità pubbliche competenti nonché in caso di verifiche e controlli interni, relativi alle previsioni della Guideline "Privacy e Data Protection" e al GDPR.

Tutte le attività sono svolte sempre d'intesa con il o con Process Owner e, ove necessario, con il supporto della funzione "LEGAL AND COMPLIANCE".

Il Delegato del Titolare procede via e-mail alla nomina del Data Record Owner individuato, inviando l'atto di nomina alla funzione "HR AND SERVICES" e alla funzione "LEGAL AND COMPLIANCE" per l'aggiornamento del Registro dei trattamenti.

Per le Società Controllate, la funzione HR competente propone alla funzione "LEGAL AND COMPLIANCE" l'individuazione dei Data Record Owner tra i primi/secondi riporti di MD/AD per competenza di processo o di compliance, ove presenti e sentite le competenti funzioni societarie.

6.5. Persone Autorizzate al Trattamento

Per effetto della presente Guideline, tutte le Persone SeaCorridor che, a qualsiasi titolo, nell'ambito delle proprie prestazioni lavorative, svolgano operazioni in relazione ad uno o più Trattamenti di Dati, sono designate Persone Autorizzate in relazione a tali Trattamenti.

La Persona Autorizzata effettua le operazioni di Trattamento attinenti all'attività lavorativa di propria competenza attenendosi alle istruzioni (di seguito "Istruzioni") impartite per lo specifico Trattamento a cui si riferiscono le operazioni medesime.

Le Istruzioni definiscono, per ciascun Trattamento o insieme di Trattamenti, le regole che le Persone Autorizzate al Trattamento hanno l'obbligo di seguire scrupolosamente per assicurare che tale Trattamento sia svolto in conformità alla presente Guideline.

Le Istruzioni si distinguono in *generali e specifiche*:

Le Istruzioni *generali* sono rese disponibili a tutte le Persone Autorizzate e immediatamente applicabili alle stesse, mediante pubblicazione in apposite sezioni del sistema in cui vengono pubblicati gli strumenti normativi (nell'ipotesi in cui tale modalità di pubblicazione non possa raggiungere tutte le Persone Autorizzate, il Data Record Owner concorderà con la funzione "LEGAL AND COMPLIANCE", la forma alternativa più efficace di diffusione).

Le Istruzioni *generali* possono essere integrate con Istruzioni specifiche (riferite cioè al Trattamento per aree specifiche o su tematiche specifiche) dai Data Record Owner, con il supporto della funzione "HR AND SERVICES" e della funzione "LEGAL AND COMPLIANCE", in relazione a ciascun singolo Trattamento o insieme di Trattamenti che presentino sufficienti elementi di omogeneità[19], ogni volta che ciò risulti opportuno.

Le Istruzioni *specifiche*, in coerenza con le Istruzioni *generali*, sono pubblicate nel sistema in cui vengono pubblicati gli strumenti normativi o diffuse con altre modalità che ne garantiscano la conoscenza tra tutte le Persone di SeaCorridor interessate.

È responsabilità di tutte le Persone di SeaCorridor condurre i Trattamenti nel rispetto delle Istruzioni Generali e Specifiche.

[19] A titolo esemplificativo possono essere considerati omogenei quei trattamenti che prevedono l'utilizzo di strumenti simili per raccogliere le stesse tipologie di dati per le identiche finalità; si pensi ad esempio ai sistemi di videosorveglianza installati presso ambienti analoghi (uffici, stabilimenti industriali, data center) oppure Trattamenti dei Dati dei dipendenti su specifici applicativi in ambito HR, Trattamenti dei Dati dei Clienti, etc.).

6.6. Responsabile per la protezione dei Dati Personali (DPO - Data Protection Officer)

Il DPO è nominato dal Delegato del Titolare di SeaCorridor d'intesa con la funzione "HR AND SERVICES" e svolge, di norma, le sue funzioni anche nell'interesse delle Società Controllate che rientrano nell'ambito di applicazione della presente Guideline.

Il Delegato del Titolare di ciascuna Società Controllata ha in ogni caso la facoltà di decidere, ove lo ritenga opportuno in termini di miglioramento dell'efficienza ed efficacia della funzione del DPO e in ragione delle specificità della Società di cui trattasi, di nominare, previa consultazione con il Delegato del Titolare di SeaCorridor, un proprio DPO appositamente preposto alle attività di Trattamento dei Dati della Società Controllata.

Il DPO svolge una funzione di garanzia della conformità della circolazione e della protezione dei Dati Personali secondo quanto stabilito dalla presente Guideline e, più in generale, dal GDPR.

Nella designazione del DPO, il Delegato del Titolare deve assicurare l'indipendenza, la professionalità e la conoscenza specialistica della normativa e delle prassi in materia di protezione dei Dati, nonché della capacità di assolvere i compiti ad esso assegnati dal GDPR.

Le responsabilità attribuite al DPO sono, a titolo esemplificativo e non esaustivo:

- informare e fornire consulenza in materia di tutela dei Dati Personali, sia per SeaCorridor, sia per le Società Controllate, interagendo con i rispettivi Delegati del Titolare, ovvero con i Data Record Owner, nonché, ove opportuno, direttamente con i responsabili delle funzioni aziendali che eseguono i Trattamenti;
- sorvegliare, in coordinamento con le competenti unità della funzione "LEGAL AND COMPLIANCE", l'osservanza della Guideline ovvero, più in generale, delle previsioni del GDPR e delle altre disposizioni, anche regolamentari, e provvedimenti dell'Autorità di Controllo applicabili in tema di protezione dei Dati Personali;
- cooperare con l'Autorità di Controllo per tutte le questioni rilevanti quali consultazioni preventive, ispezioni/procedimenti, Richieste, reclami e/o segnalazioni;
- fornire supporto in relazione ai temi connessi alla Violazione dei Dati Personali, anche ai fini della presentazione delle eventuali notifiche obbligatorie ai sensi del GDPR, operando con l'assistenza specialistica della funzione "HR AND SERVICES";
- nell'esecuzione del Data Protection Impact Assessment, fornire pareri, ove richiesto, ai Data Record Owner[20] che provvedono a informare le funzioni coinvolte.

Il DPO adotta specifico regolamento al fine di disciplinare le funzioni, le prerogative e le regole necessarie al suo corretto funzionamento.

Il DPO, per lo svolgimento efficace dei compiti assegnatigli dalla legge, ha facoltà di richiedere la collaborazione di tutte le funzioni aziendali di SeaCorridor e delle Società Controllate.

[20] All'esito della DPIA, il DPO riceve, per il tramite della Segreteria tecnica del DPO, il report di chiusura e la nota di supporto inviata dal Data Record Owner per la propria valutazione.

6.7. Amministratore di sistema

Per i sistemi gestiti all'interno della funzione "HR AND SERVICES", l'Amministratore di Sistema di norma verifica e documenta la sussistenza dei seguenti requisiti:

- competenza in ambito informatico, anche in relazione a tematiche inerenti al profilo della sicurezza, ad esempio in considerazione del percorso formativo e/o dell'esperienza professionale maturata;
- conoscenza delle disposizioni normative e aziendali in materia di Trattamento di Dati Personali.

Per le Società Controllate che non hanno accentrato le attività nella funzione "HR AND SERVICES" di SeaCorridor e che effettuano una gestione diretta dei propri sistemi informatici, la nomina dell'Amministratore di Sistema viene effettuata dal Data Record Owner.

6.8. Funzione "LEGAL AND COMPLIANCE"

La funzione "LEGAL AND COMPLIANCE" è l'unità organizzativa, responsabile di presidiare le evoluzioni normative in materia di privacy e data protection, di fornire assistenza specialistica a tutte le funzioni aziendali di competenza, di volta in volta interessate, di SeaCorridor e delle Società Controllate e di garantire il coordinamento con le unità di compliance eventualmente operanti nelle società stesse.

Le funzioni "LEGAL AND COMPLIANCE" Controllate, ove esistenti, assicurano inoltre i flussi informativi verso la funzione "LEGAL AND COMPLIANCE" di SeaCorridor circa l'avvio e lo stato delle istruttorie e dei procedimenti davanti alle autorità competenti per gli ambiti di compliance presidiati e in ogni caso in cui siano riscontrati punti di attenzione, anche potenziali, relativi al sistema di controllo interno e gestione dei rischi di compliance.

- Inoltre, la funzione "LEGAL AND COMPLIANCE": svolge il ruolo di segreteria tecnica del DPO provvedendo alla gestione dei flussi informativi e/o di altra natura fra il DPO e le funzioni aziendali di volta in volta interessate e/o i terzi. Ciò anche nell'ipotesi in cui, nell'ambito di una o più Società Controllate siano istituiti specifici DPO;
- garantisce, per quanto di competenza, le iniziative di formazione in materia di privacy e data protection;
- riesamina periodicamente il sistema di compliance previsto nella presente Guideline anche sulla base delle risultanze delle attività di risk assessment, monitoraggio e di audit e delle best practice di riferimento, e formula proposte di miglioramento del sistema stesso.

6.9. Responsabile del Trattamento esterno

Il soggetto terzo o altra Società Controllata di SeaCorridor che svolga per SeaCorridor o Società Controllata attività in appalto/outsourcing, che comportino il Trattamento di Dati Personali di cui SeaCorridor o Società Controllata siano Titolare, deve essere nominato dallo stesso procuratore che sottoscrive il contratto o che conferisce l'incarico quale Responsabile del Trattamento esterno. La clausola contrattuale relativa alla predetta nomina, come meglio dettagliato nell'apposita sezione del sistema in cui vengono pubblicati gli strumenti normativi, prevede, tra l'altro, l'impegno della

controparte contrattuale (ad esempio fornitori, appaltatori, subappaltatori) al rispetto dei criteri, finalità e modalità di Trattamento dei Dati Personali previsti dal GDPR e da eventuali istruzioni impartite dal committente, nonché controlli e vigilanza specifica sulle attività del Responsabile del Trattamento esterno. L'elenco dei Responsabili del Trattamento esterno è contenuto in apposita sezione del Registro delle Attività di Trattamento.

7. Linee guida per la tutela dei dati personali

7.1. Approccio risk-based

I Dati Personali devono essere trattati per scopi leciti e trasparenti, senza eccedere le finalità per le quali siano stati raccolti, in conformità all'informativa privacy fornita ai soggetti interessati e nel rispetto del consenso da questi espresso, ove necessario. Il Trattamento dei Dati Personali deve avvenire in base a regole definite in funzione del grado di rischio cui sono esposte le attività a cui i trattamenti afferiscono.

A titolo esemplificativo e non esaustivo sono individuate le seguenti attività a rischio:

- rapporti con clienti;
- rapporti con i fornitori;
- rapporti con business partner (tra cui i consulenti, i broker, JV, partnership commerciali);
- compravendita e affitto di aziende/rami di azienda e altri complessi di beni/acquisizione o cessione di partecipazioni sociali che possono determinare il trasferimento di Dati Personali;
- rapporti afferenti alle attività con/su social media;
- rapporti con i dipendenti e candidati (tra cui anche i rapporti di collaborazione coordinata e continuativa);
- richieste dell'Autorità.

Il livello di rischio associato alle succitate attività e ai trattamenti da esse scaturenti viene determinato ad esito delle attività di risk assessment condotte sulla base del processo di Compliance Integrata.

In funzione degli esiti di tale attività vengono determinate, con un approccio *risk-based*, le eventuali azioni in concreto necessarie a garantire, in relazione alle varie attività a rischio, il rispetto della normativa applicabile e i principi di riferimento riportati nella presente Guideline.

I Trattamenti sono eseguiti tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del Trattamento stesso, nonché dei rischi rilevanti per gli Interessati. In particolare, nell'ambito di qualsiasi iniziativa, i sistemi informativi utilizzati e i processi adottati devono soddisfare i principi della protezione dei dati fin dalla progettazione (c.d. *privacy by design*) e per impostazione predefinita (c.d. *privacy by default*).

7.2. Privacy by Design e valutazione dei rischi

7.2.1. Aspetti generali

Il GDPR stabilisce che la privacy e data protection debba essere considerata nelle valutazioni preliminari di ogni nuova attività, progetto, iniziativa e/o servizio avviato da SeaCorridor o dalle Società Controllate *(Privacy by Design*).

In un'ottica di *Privacy by Design,* il Data Record Owner deve confrontarsi con la funzione "LEGAL AND COMPLIANCE e verificare quale sia la Base Giuridica che legittimi il Trattamento.

Il Trattamento può essere effettuato soltanto quando sia legittimato da almeno una delle seguenti Basi Giuridiche:

i. consenso inequivoco dell'interessato;
ii. esecuzione del contratto concluso con l'interessato[21];
iii. adempimento di un obbligo previsto da specifiche normative esterne a cui è soggetto il Titolare;
iv. salvaguardia di un interesse vitale dell'Interessato;
v. esecuzione di un compito di interesse pubblico da parte del Titolare;
vi. perseguimento di un interesse legittimo del Titolare.

I Trattamenti di cui alla precedente punto vi) sono effettuati a seguito di una valutazione comparativa (Legitimate Interest Assessment, di seguito "LIA") tra l'interesse legittimo del Titolare e i diritti, gli interessi o le libertà fondamentali dell'Interessato e a condizione che questi ultimi non prevalgano sull'interesse del Titolare.

La funzione "LEGAL AND COMPLIANCE" supporta il Data Record Owner, nell'esecuzione della LIA, ogni qualvolta il legittimo interesse sia posto alla base di un Trattamento. Il Data Owner e il Process Owner interessato devono altresì documentare le ragioni a favore della scelta di questa Base Giuridica, compresi i motivi per cui non è possibile utilizzare le altre[22].

Il Data Owner ha cura di adottare misure di sicurezza idonee alla tipologia e al grado di rischio del Trattamento connesso all'attività/progetto o iniziativa e definisce le modalità di monitoraggio delle stesse, d'intesa con la funzione "LEGAL AND COMPLIANCE" e in coordinamento con la funzione "HR AND SERVICES" competente, e con le funzioni o aree aziendali eventualmente coinvolte.

7.2.2. Valutazione preliminare di impatto privacy

La valutazione preliminare di impatto privacy (di seguito "Pre-DPIA") di attività/progetti o iniziative (di seguito, "Attività") che possano comportare Trattamenti di Dati Personali deve essere garantita dal Data Owner, con il supporto della funzione "LEGAL AND COMPLIANCE" in materia di risk assessment già nella fase iniziale o di ideazione/pianificazione dell'Attività, con congruo anticipo rispetto all'avvio della stessa e, comunque, prima dell'inizio del Trattamento.

A seguito della valutazione preliminare effettuata:

- se il Trattamento è già presente nel Registro o, comunque, è simile[23] rispetto ad un Trattamento già esistente, il Data Record Owner competente, tiene traccia – anche tramite il

[21] Per tale si intende anche l'esecuzione di misure precontrattuali adottate su richiesta dell'Interessato (es. invio *curriculum vitae*, contatto con servizio clienti per richiedere informazioni per la stipula di un nuovo contratto etc.).
[22] Si veda il Considerando 69 del Regolamento che recita «*È opportuno che incomba al Titolare del trattamento dimostrare che i suoi interessi legittimi cogenti prevalgono sugli interessi o sui diritti e sulle libertà fondamentali dell'interessato*».
[23] Un Trattamento è simile ad un altro già esistente quando, ad esempio, la categoria di dati trattati è la medesima (es. accesso tramite rilevazione dell'impronta digitale o tramite la lettura dell'iride).

verbale di pre-DPIA – di tali valutazioni e procede nell'Attività, senza modificare/aggiornare il Registro.

- se il Trattamento è nuovo[24], il Data Record Owner competente, che coinvolge l'Unità "LEGAL AND COMPLIANCE", raccoglie le informazioni necessarie ad alimentare il Registro dei trattamenti.
- Se il Trattamento si sostanzia in una modifica di un Trattamento già esistente[25], si applica quanto previsto al precedente punto 2.

Qualora dagli esiti della Pre-DPIA emerga che non è necessario procedere ad una DPIA[26], il Data Record Owner tiene traccia delle valutazioni effettuate, di norma tramite un verbale di Pre-DPIA, e procede con le attività di Trattamento.

Al ricorrere anche solo di uno dei criteri di Pre-DPIA[27] indicati nel questionario di assessment, si procede alla Valutazione di impatto privacy, di cui al successivo paragrafo.

7.2.3. Valutazione d'Impatto (Data Protection Impact Assessment o DPIA)

Il Data Record Owner, con il supporto della funzione "LEGAL AND COMPLIANCE" , effettua, in occasione di modifiche sostanziali al Trattamento dei Dati, la DPIA, tenendo traccia degli esiti. La DPIA contiene almeno:

- la descrizione sistematica dei Trattamenti previsti e delle finalità degli stessi, compreso, ove applicabile, l'indicazione dell'interesse legittimo perseguito dal Titolare;
- la valutazione della necessità e proporzionalità dei Trattamenti in relazione alle finalità;
- la valutazione dei rischi per i diritti degli Interessati;
- le misure di sicurezza e i meccanismi per garantire la protezione dei Dati Personali in conformità al GDPR.

All'esito della DPIA, il Data Record Owner competente con il supporto della funzione "LEGAL AND COMPLIANCE", elabora la scheda sintetica che, insieme al Verbale di Pre-DPIA e alla nota di chiusura, viene trasmessa al DPO.

Nel caso in cui il risultato della DPIA indichi che il Trattamento non presenta criticità, il DPO comunica al Data Record Owner di riferimento, per il tramite della Segreteria Tecnica, che si può procedere al Trattamento.

---

[24] Es. è il caso dell'utilizzo di nuove tecnologie o di modalità innovative di business (e-commerce; utilizzo dei social o, comunque, di canali "non convenzionali" nei rapporti con clienti, etc.)

[25] Qualsiasi trattamento di dati le cui condizioni di attuazione (ambito di applicazione, finalità, dati personali raccolti, identità dei titolari del trattamento o dei destinatari, periodo di conservazione dei dati, misure tecniche e organizzative, ecc.) siano mutate rispetto alla prima individuazione e che possano presentare un rischio elevato a valle della PRE-DPIA, devono essere soggette a una valutazione d'impatto.

[26] In base ai criteri definiti nel Provvedimento del Garante "Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679" dell'11 ottobre 2018.

[27] I criteri di PRE-DPIA sono integrati nel questionario di assesment nel registro dei trattamenti.

Laddove il risultato della DPIA indichi che il Trattamento possa presentare un rischio elevato, il DPO, per il tramite della Segreteria Tecnica, chiede al Data Record Owner di valutare se:

- adottare misure correttive idonee a mitigare il rischio; in tal caso, gli interventi di adeguamento a mitigazione del rischio vengono sottoposti di nuovo all'approvazione del DPO o
- chiedere al Delegato del Titolare di procedere alla consultazione preventiva dell'Autorità di Controllo, per ottenere indicazioni su come gestire l'eventuale rischio. In tal caso, il Delegato del Titolare comunica all'Autorità di Controllo, secondo quanto previsto dalla normativa privacy.

7.3. Conservazione e sicurezza del Dato Personale

7.3.1. Conservazione dei Dati Personali (c.d. data retention)

I Dati Personali sono conservati in una forma che consenta l'identificazione degli Interessati per un arco di tempo funzionale al conseguimento delle finalità per le quali sono raccolti e trattati. Al conseguimento delle finalità per i cui Dati sono raccolti e trattati, di norma questi stessi devono essere distrutti e/o de-identificati; tuttavia i Dati Personali possono essere conservati per periodi più lunghi a condizione che vi sia il consenso espresso dell'Interessato, oppure ciò sia consentito da una norma di legge, oppure siano conservati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici o che venga effettuata una LIA.

Il Data Record Owner, con il supporto della funzione "LEGAL AND COMPLIANCE", stabilisce il tempo di conservazione dei Dati in relazione alle finalità di ciascun Trattamento, se non già individuato nel relativo strumento normativo applicabile in materia, e ne assicura l'annotazione nel Registro.

7.3.2. Misure di sicurezza

Il Data Record Owner in collegamento con il supporto della funzione "LEGAL AND COMPLIANCE" e della funzione "HR AND SERVICES" valuta il livello di sicurezza.

Nel valutare l'adeguato livello di sicurezza, il Data Record Owner, con il supporto della funzione "LEGAL AND COMPLIANCE" e della funzione "HR AND SERVICES" sentito ove necessario il Process Owner interessato, tiene conto dei rischi derivanti dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, di Dati Personali trasmessi, conservati o comunque trattati.

A seguito della valutazione del livello di sicurezza, sentita la funzione "LEGAL AND COMPLIANCE", il Data Record Owner di riferimento, propone al Process Owner l'adozione di misure tecniche e organizzative adeguate per garantire un livello di sicurezza proporzionato al rischio dei Trattamenti, che possono comprendere:

a. ove applicabile la pseudonimizzazione[28] e la crittografia dei Dati Personali;
b. la protezione delle informazioni aziendali trattate al di fuori delle applicazioni informatiche;
c. misure volte ad assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di Trattamento;
d. misure volte a ripristinare tempestivamente la disponibilità e l'accesso dei Dati Personali in caso di incidente fisico o tecnico;

a) modalità operative per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del Trattamento.

7.3.3. Denuncia di Violazione dei Dati Personali – (Data Breach)

Tutte le Persone di SeaCorridor possono accedere ai Dati oggetto dei Trattamenti esclusivamente per quanto strettamente funzionali all'adempimento delle proprie prestazioni lavorative, nel rispetto della presente Guideline e delle Istruzioni. Un accesso ai Dati al di fuori di quanto strettamente necessario ad adempiere alle proprie prestazioni e/o comunque non conforme alle Istruzioni deve essere considerato una Violazione dei Dati Personali ai fini della presente Guideline e potrà conseguentemente essere sanzionato anche sul piano disciplinare.

Le Persone di SeaCorridor devono agire con la massima diligenza al fine di prevenire episodi di Violazione dei Dati Personali, ossia accessi non autorizzati -da parte di altre Persone di SeaCorridor e/o terzi- ai Dati oggetto dei Trattamenti facenti capo a SeaCorridor o comunque incidenti al corretto svolgimento dei Trattamenti medesimi.

Inoltre, fermo restando quanto previsto dalla Guideline "Segnalazioni, anche anonime, ricevute da SeaCorridor e da Società Controllate" di SeaCorridor, chiunque venga a conoscenza, direttamente e/o indirettamente (i.e. su indicazione di un Incaricato, di una Persona di SeaCorridore/o di un terzo) di una possibile Violazione di Dati Personali (i.e. anche solo sospettata) -quale che sia la possibile fonte/origine di tale Violazione (Terzi, Persone di SeaCorridor, fonte non identificata, evento accidentale)- deve comunicare immediatamente tale possibile Violazione, unicamente tramite l'indirizzo email Data_breach@sea-corridor.com[29], al DPO ove nominato ai sensi della presente Guideline e al Data Record Owner competente, ove noto.

A seguito della ricezione della comunicazione di una possibile Violazione di Dati Personali, la funzione "LEGAL AND COMPLIANCE" coinvolge la funzione "HR AND SERVICES".

Le funzioni aziendali come sopra identificate a seguito di tempestiva consultazione, valuteranno congiuntamente se ricorrono effettivamente i presupposti per considerare l'evento come Violazione di Dati Personali e, ove possibile, quale ne sia la portata e le caratteristiche, con specifica attenzione ai

[28] Trattamento dei Dati Personali in modo tale che gli stessi 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

[29] La gestione della mail box è affidata alla funzione "LEGAL AND COMPLIANCE".

rischi per i diritti e le libertà degli Interessati i cui Dati siano stati oggetto della Violazione. In particolare, si valuterà se ricorrano o meno le circostanze che, in coerenza con la normativa applicabile, rendono necessario o opportuno informare dell'avvenuta Violazione l'Autorità di Controllo e/o gli Interessati i cui Dati siano stati oggetto della Violazione.

Sarà cura della funzione "LEGAL AND COMPLIANCE" trasmettere via e-mail al Data Record Owner di riferimento, che informerà le altre funzioni eventualmente coinvolte, una relazione contenente le conclusioni di tali valutazioni. Tale relazione viene altresì inviata alla funzione "LEGAL AND COMPLIANCE" in tutti i casi in cui la Violazioni riguardi Dati Personali di Società Controllate in cui sia presente un presidio specialistico in materia di privacy.

Qualora sia stata accertata una Violazione dei Dati Personali, la relazione sarà inviata anche al DPO e al Delegato del Titolare che, sulla base di quanto indicato, provvederà alla notifica della Violazione all'Autorità di Controllo e/o agli Interessati, secondo i termini definiti dalla normativa di riferimento.

7.4. Registri delle attività di Trattamento

Ogni società detiene uno o più Registri delle attività di Trattamento, che vengono redatti e aggiornati da ogni Data Record Owner e contengono informazioni relative:

- all'elenco dei trattamenti eseguiti nell'area di competenza;
- alla Base Giuridica che legittima il Trattamento
- alle finalità del Trattamento;
- alle categorie di Interessati e di Dati Personali;
- ai destinatari a cui i Dati sono o saranno comunicati;
- ad eventuali Trasferimenti, insieme all'indicazione delle garanzie adeguate;
- ai Responsabili esterni del Trattamento nominati;
- ai termini ultimi previsti per la cancellazione delle diverse categorie di Dati oppure, ove non possibile, ai criteri per determinare tali termini;
- alle misure di sicurezza.

I Data Record Owner devono aggiornare i Registri delle attività di Trattamento per cui sono stati individuati:

1. in caso emerga la necessità di effettuare un nuovo Trattamento nel corso dell'anno e
2. in occasione della cd. "campagna di aggiornamento del Registro", promossa dalla funzione "LEGAL AND COMPLIANCE" a cadenza di norma biennale.

7.5. Reportistica Privacy

7.5.1. Reportistica a cura del Data Record Owner

Entro il 31 dicembre di ciascun anno ogni Data Record Owner trasmette alla funzione "LEGAL AND COMPLIANCE" una lettera di attestazione contenente almeno le seguenti indicazioni in merito ai trattamenti ricadenti nella propria sfera di operatività effettuati nel corso dell'anno di riferimento:

- nuovi trattamenti;
- interventi di modifica/aggiornamento delle Istruzioni o redazione di nuove Istruzioni;
- elenco dei progetti sottoposti a Data Protection Impact Assessment;
- elenco delle iniziative formative in materia di privacy alle quali ha preso parte come docente e/o come discente;
- elenco delle Violazioni e/o degli episodi di sospetta Violazione;
- interventi di modifica delle misure di sicurezza;
- richieste/Reclami da parte di Interessati ricadenti nella sua sfera di operatività;

In caso di dubbi su contenuti specifici da inserire nella lettera di attestazione/reportistica, il Data Record Owner si avvale del supporto della funzione "LEGAL AND COMPLIANCE" e/o della competente funzione "HR AND SERVICES".

7.5.2. Reportistica a cura del DPO

Il DPO riferisce al Delegato del Titolare attraverso la redazione di una relazione annuale sulle attività svolte e sulle questioni in merito alle quali è stato coinvolto. La relazione comprende anche le questioni di maggior rilevo che abbiano interessato le singole Società Controllate. Nell'eventualità che una o più Società Controllate, sulla base di quanto previsto al paragrafo 6.3, abbiano costituito un loro proprio DPO, quest'ultimo dovrà inviare la sua relazione al DPO di SeaCorridor affinché quest'ultimo possa tenerne conto ai fini della propria relazione. A tal fine il DPO di SeaCorridor definirà le relative scadenze.

7.6. Trasferimento Dati verso Paesi extra-UE

Il Trasferimento di Dati verso Paesi extra UE è consentito solo in presenza di specifiche garanzie in merito al rispetto dei Diritti dell'Interessato. Pertanto, il Data Record Owner competente per il Trattamento oggetto di Trasferimento, dovrà consultare la funzione "LEGAL AND COMPLIANCE" già nella fase di ideazione/pianificazione e, in ogni caso, prima della realizzazione delle Attività che prevedano il Trasferimento.

In particolare, ogni volta che SeaCorridor o una Società Controllata, in qualità di Titolare del Trattamento, intenda effettuare un Trasferimento di Dati Personali dall'Unione Europea verso un Paese extra-UE, è necessario verificare se il Trasferimento rientri una delle seguenti ipotesi di deroga al divieto:

- il Trasferimento di Dati Personali è diretto verso un Paese ricompreso nell'elenco dei Paesi che, ai sensi di una decisione di adeguatezza della Commissione Europea, presenta un livello di protezione adeguato tale da fornire idonee garanzie per i Diritti dell'Interessato[30];

[30] Al momento della pubblicazione della presente Guideline, la Commissione Europea ha emanato decisioni di adeguatezza rispetto ai seguenti Paesi: Andorra, Argentina, Canada, Faer Oer, Guernsey, Isola di Man, Israele, Jersey, Nuova Zelanda, Svizzera, Uruguay. L'elenco aggiornato dei Paesi che forniscono adeguato livello di protezione dei Dati Personali è sempre consultabile al seguente link http://www.garanteprivacy.it/home/provvedimenti-normativa/normativa/normativa-comunitaria-e-intenazionale/trasferimento-dei-dati-verso-paesi-terzi.

- il Trasferimento di Dati Personali è disciplinato a livello contrattuale tra le parti tramite l'inserimento di apposite clausole standard adottate dalla Commissione Europea i cui contenuti sono disponibili in apposita sezione del sistema in cui vengono pubblicati gli strumenti normativi.

Il Trasferimento dei Dati diretto verso gli USA o altro Paese fuori dall'Unione Europea per il quale non è stata emanata dalla Commissione Europea una decisone di adeguatezza renderà necessario individuare adeguate misure supplementari finalizzate a garantire un livello di protezione sostanzialmente equivalente a quello garantito dal diritto dell'Unione Europea. I contenuti di tali misure supplementari (meccanismi di controllo o clausole contrattuali rafforzative rispetto allo standard adottato dalla Commissione), saranno disponibili in apposita sezione del sistema in cui vengono pubblicati gli strumenti normativi.

Tali misure trovano applicazione anche laddove l'importatore dei Dati sia una Società Controllata.

8. Linee guida in materia di contratti e rapporti con gli interessati

8.1. Privacy e contratti

Tutti i contratti che comportino il Trattamento di Dati Personali devono contenere apposite clausole volte a regolamentare gli aspetti rilevanti per la privacy. A tal fine sono rese disponibili in apposita sezione del sistema in cui vengono pubblicati gli strumenti normativi le clausole standard da applicare da parte delle funzioni aziendali competenti per la stesura del contratto[31]. Nel caso si renda necessario apportare modifiche sostanziali alle clausole stesse dovrà essere consultata la funzione "LEGAL AND COMPLIANCE".

Qualora il rapporto contrattuale comporti il Trattamento, da parte della controparte[32], di Dati Personali nella titolarità o contitolarità[33] di SeaCorridor, è necessario che la controparte stessa sia designata Responsabile Esterno del Trattamento[34].

Il Responsabile Esterno del Trattamento dovrà effettuare i trattamenti in nome e per conto della società di SeaCorridor, sulla base di istruzioni scritte definite nel contratto ed è vincolato al rispetto delle stesse.

8.2. Informativa all'interessato

Le operazioni di Trattamento devono essere svolte nel rispetto di quanto previsto nell'Informativa all'Interessato.

L'Informativa deve contenere tutte le informazioni necessarie a garantire che l'Interessato sia consapevole dei contenuti del Trattamento relativo ai suoi Dati Personali. Nell'Informativa devono pertanto essere indicati la Base Giuridica del Trattamento, le finalità del Trattamento, le modalità dello stesso, le categorie di soggetti interni ed esterni ad Eni che avranno accesso ai Dati dell'Interessato, il tempo di conservazione dei Dati, gli estremi identificativi del Titolare del Trattamento, i Dati di contatto del DPO, se i Dati sono trasferiti oltre il territorio UE, se viene effettuata una profilazione con i Dati

[31] Nel caso di contratti stipulati da funzioni centralizzate diverse dalle unità richiedenti, la clausola privacy da inserire all'interno del contratto viene definita col supporto dell'unità richiedente e con l'eventuale supporto della funzione compliance privacy.

[32] A titolo esemplificativo e non esaustivo: i) Esternalizzazione del servizio di storage e archiviazione dati del personale; ii) Servizi di cloud. Tuttavia, anche altri progetti, che ad un primo impatto potrebbero sembrare non particolarmente rilevanti per la privacy, implicano trattamenti di dati, ad esempio: i) Esternalizzazione servizi di payroll; ii) Implementazione software pubblicità comportamentale; iii) Servizi di facility management iv) Piattaforma per la gestione dei flexible benefit dei dipendenti ecc.

[33] Nei casi in cui la controparte effettui in maniera autonoma il trattamento dei dati, la stessa agirà in veste di autonomo Titolare del Trattamento. Laddove, invece le finalità e i mezzi del trattamento sono stabiliti congiuntamente tra la controparte e la società di SeaCorridor, vi sarà un rapporto di contitolarità. Per determinare correttamente lo scenario applicabile, è necessario fare attenzione ai flussi, alle modalità del trattamento e alle caratteristiche delle attività oggetto del contratto.

[34] È il caso, ad esempio, dei contratti con gli operatori di call-center; dell'esternalizzazione di alcuni servizi per la gestione delle buste paga dei dipendenti; etc.

dell'Interessato, del diritto di revocare il consenso prestato nei casi in cui il Trattamento è svolto sulla base del consenso dell'Interessato (v. sotto), nonché di ogni altro Diritto dell'Interessato.

L'Informativa deve essere fornita prima dell'inizio dell'attività di Trattamento se i Dati sono raccolti direttamente presso l'Interessato e prima dell'espressione del Consenso (se e quando richiesto) ovvero al primo contatto utile[35] con l'Interessato, se i Dati sono raccolti presso terzi.

Le funzioni competenti che attivano la raccolta di Dati Personali sono tenute a rilasciare specifiche Informative:

- ai dipendenti all'atto dell'assunzione36, a cura delle funzioni HR competenti;
- ai collaboratori37 all'inizio della collaborazione a cura delle funzioni HR competenti;
- ai terzi fornitori, all'atto della richiesta di offerta, a cura delle unità approvvigionamenti competenti;
- ai consulenti, a cura della funzione incaricata di gestire il rapporto contrattuale;
- ai clienti e/o terzi, al momento della raccolta dei Dati Personali (es. sottoscrizione del contratto) a cura delle unità competenti (es. unità di vendita) ovvero raccolti attraverso altre forme di vendita diretta tramite telefono o via web;
- a tutti gli altri soggetti terzi non rientranti nelle categorie sopra riportate per i quali sia necessario raccogliere e trattare Dati Personali che li riguardino, alla prima occasione disponibile di contatto con SeaCorridor, a cura della funzione incaricata di gestire tale contatto38;
- a tutti gli utenti dei siti Internet gestiti da SeaCorridor e dalle Società Controllate, anche in relazione al Trattamento dei Dati tramite cookie e altri strumenti di profilazione, a cura della funzione competente per la gestione del sito e in collaborazione con le altre competenti funzioni di SeaCorridor, quali "HR AND SERVICES".

8.3. Consenso dell'Interessato

Tra le Basi Giuridiche che legittimano il Trattamento di Dati Personali[39] rientra il Consenso espresso da ciascun Interessato al Trattamento dei propri Dati Personali.

Ove ad esito delle valutazioni di impatto privacy, per un determinato Trattamento fosse richiesto il Consenso dell'Interessato lo stesso deve essere acquisito prima dell'inizio del Trattamento. Il Consenso dell'Interessato deve essere libero (quindi non condizionato da situazioni che potrebbero obbligare l'Interessato a fornirlo), espresso (quindi fornito in maniera inequivocabile), informato (quindi fornito a seguito dell'Informativa) e modulare (ossia riferito alle singole e specifiche modalità e finalità del

[35] Per contatto utile si intende, a titolo esemplificativo, la chiamata per finalità di marketing/promozionale successiva al rilascio del consenso da parte dell'interessato ad essere contattato per tali finalità.
[36] A seguito dell'assunzione, eventuali aggiornamenti delle informative privacy per i dipendenti italiani saranno comunicati tramite apposita piattaforma; per i dipendenti UE, tramite e-mail.
[37] Ai fini delle presenti Istruzioni si intendono i collaboratori coordinati e continuativi.
[38] Ad esempio, amministratori, sindaci, revisori, componenti degli Organi di Controllo e Organismi di Vigilanza istituiti ai sensi del d.lgs. 231/2001 nonché azionisti che si recano all'assemblea.
[39] Si veda quanto riportato al paragrafo 7.2.1.

Trattamento per cui la legge impone la richiesta del consenso: i.e. marketing; profilazione[40] etc.). L'effettiva acquisizione del Consenso dell'Interessato con le caratteristiche sopra elencate deve essere verificata dalla funzione aziendale cui fa capo il Trattamento.

8.4. Diritti dell'Interessato

SeaCorridor assicura il rispetto dei Diritti dell'Interessato, ponendo in essere le iniziative utili ad un effettivo ed agevole esercizio di tali diritti a tutti gli Interessati.

Qualora un Interessato formuli richieste/Reclami nell'esercizio dei propri Diritti, il Data Record Owner cui fa capo il Trattamento a cui si riferiscono le richieste/i Reclami, si attiva prontamente per dare seguito agli stessi, richiedendo il supporto alla funzione "HR AND SERVICES" e/o della funzione "LEGAL AND COMPLIANCE" nel caso di dubbi sull'effettiva portata dei diritti medesimi e sulle modalità del loro esercizio.

[40] Qualsiasi forma di Trattamento automatizzato di Dati Personali consistente nell'utilizzo di questi 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.

9. Formazione

Al fine di garantire la diffusione, all'interno dell'azienda, di una "cultura della privacy", e di fornire gli strumenti adeguati per assicurare il rispetto della normativa in materia di Dati Personali, la funzione "LEGAL AND COMPLIANCE" definisce i programmi della formazione obbligatoria, secondo l'approccio "risk-based". Contenuti, modalità e frequenza della formazione sono pertanto calibrati rispetto al livello di esposizione al rischio delle Persone SeaCorridor, in funzione delle attività svolte o della famiglia professionale di appartenenza.

10. Monitoraggio e controlli

10.1. Monitoraggio di secondo secondo livello

In coerenza con quanto previsto disposizioni applicabili in materia di compliance, l'attività di compliance monitoring è finalizzata a rilevare ed analizzare periodicamente l'andamento dei rischi di compliance attraverso lo svolgimento di specifici controlli e l'analisi di indicatori di rischio volti ad assicurare l'aderenza ai requisiti normativi e l'efficacia dei modelli posti a presidio dei rischi di Compliance.

Le attività di compliance monitoring in materia di privacy, sono pianificate ed effettuate secondo un approccio risk based.

A tale fine, i Data Record Owner competenti assicurano all'unità compliance competente in materia di monitoring la disponibilità delle informazioni necessarie alle attività di verifica da effettuare, secondo le tempistiche e le richieste documentali definite dalla medesima unità.

A conclusione delle attività di compliance monitoring, la funzione "LEGAL AND COMPLIANCE" per il monitoring predispone e condivide un rapporto di monitoraggio con le Unità competenti nonché con i Data Record Owner.

10.2. Controlli di terzo livello

La funzione "INTERNAL AUDIT" di SeaCorridor, sulla base del proprio Piano annuale di *audit* approvato dal Consiglio di Amministrazione di SeaCorridor, esaminerà e valuterà in maniera indipendente il sistema di controllo interno, al fine di verificare che sia rispettato quanto previsto dalla presente Guideline.