22 dicembre 2020

DATA PROTECTION POLICY

Modello organizzativo

Indice

DATA PROTECTION POLICY

Modello organizzativo

1 Introduzione

Il Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (Regolamento Generale sulla Protezione dei Dati e, in inglese, *General Data Protection Regulation*, di seguito, il "**GDPR**") è divenuto pienamente applicabile a decorrere dal 25 maggio 2018.

Il presente modello organizzativo ("**Modello Organizzativo**") raccoglie le misure tecniche ed organizzative che la società Falck Renewables S.p.A. ("**Società**") attua per garantire – ed essere in grado di dimostrare – la conformità al GDPR delle attività di trattamento dei dati personali delle persone fisiche effettuate direttamente o che soggetti terzi effettuano per suo conto e al fine di specificare i presidi organizzativi e di processo di cui si è dotata per garantire una tutela effettiva ed efficace dei dati personali di cui è titolare del trattamento.

2 Ambito di applicazione

Il presente Modello Organizzativo si applica agli amministratori, dirigenti, dipendenti, collaboratori, consulenti della Società, nonché ai responsabili del trattamento, fornitori e ad ogni altro soggetto terzo che effettua operazioni di trattamento di dati personali per conto della Società ("**Destinatari**").

Il presente Modello Organizzativo si applica a tutte le società controllate direttamente o indirettamente dalla Società, compresa (i) la Società, (ii) Vector Cuatro S.L.U. e le società dalla stessa controllate direttamente o indirettamente, nonché (iii) Falck S.p.A. (collettivamente, il "**Gruppo**") soggette all'applicazione del GDPR[1] e che, in coerenza con i principi di autonomia e di responsabilità proprie di ciascuna società del Gruppo, si impegnano a recepire e adottare il presente Modello Organizzativo definendo i principi di governo societario e di controllo in materia di trattamento dei dati personali in conformità al presente Modello Organizzativo.

Ogni riferimento alla Società contenuto all'interno del presente Modello Organizzativo dovrà essere inteso come rivolto a ciascuna società del Gruppo.

3 Definizioni

In aggiunta alle definizioni sopra fornite, ai fini del presente Modello Organizzativo si intende per:

- "**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;
- "**Autorità di Controllo**": l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'Art. 51 del GDPR (https://edpb.europa.eu/about-edpb/board/members_en);
- "**consenso dell'interessato**": qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante

[1] Ai sensi dell'Art. 3 del Regolamento, il Regolamento si applica (i) al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione Europea, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione Europea, nonché (ii) al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione Europea, quando le attività di trattamento riguardano: (a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione Europea, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure (b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione Europea.

dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

- "**Data Steward**": i soggetti che, individuati dal responsabile dell'unità organizzativa di appartenenza, sono chiamati a supervisionare e a sovrintendere il rispetto del Modello Organizzativo da parte dei Destinatari, assistere la Società nell'attuazione delle Policy Privacy e agire come referenti principali per le questioni in materia di trattamento di dati personali all'interno della loro unità organizzativa, nonché fungere da punto di contatto per gli interessati e i Destinatari;
- "**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 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 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;
- "**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;
- "**limitazione di trattamento**": il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- "**Normativa Privacy**": tutte le disposizioni di legge o regolamento applicabili in materia di protezione dei dati personali, ivi incluse, a titolo esemplificativo e non esaustivo, le disposizioni del GDPR e della normativa nazionale in materia di protezione di dati personali, nonché i provvedimenti e le linee guida delle Autorità di Controllo;
- "**Paesi Terzi**": paesi esterno allo Spazio Economico Europeo;
- "**Privacy Policy**": le policy e procedure adottate dalla Società al fine di regolamentare i diversi aspetti legati al trattamento dei dati personali che formano parte integrante e sostanziale del presente Modello Organizzativo, incluse, a titolo esemplificativo e non esaustivo, le policy allegate al presente Modello Organizzativo;
- "**Privacy Expert**": i soggetti designati direttamente dalla Società che, nello svolgimento delle loro funzioni e nei limiti dei poteri attribuiti, fungono da punto di contatto per i Data Steward per le questioni in materia di trattamento di dati personali e, in particolare, le questioni relative al rispetto del presente Modello Organizzativo e della Normativa Privacy da parte della Società;
- "**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;

- "**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;
- "**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;
- "**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;
- "**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;
- "**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.

Le espressioni al singolare manterranno lo stesso significato al plurale, ove il contesto lo richieda.

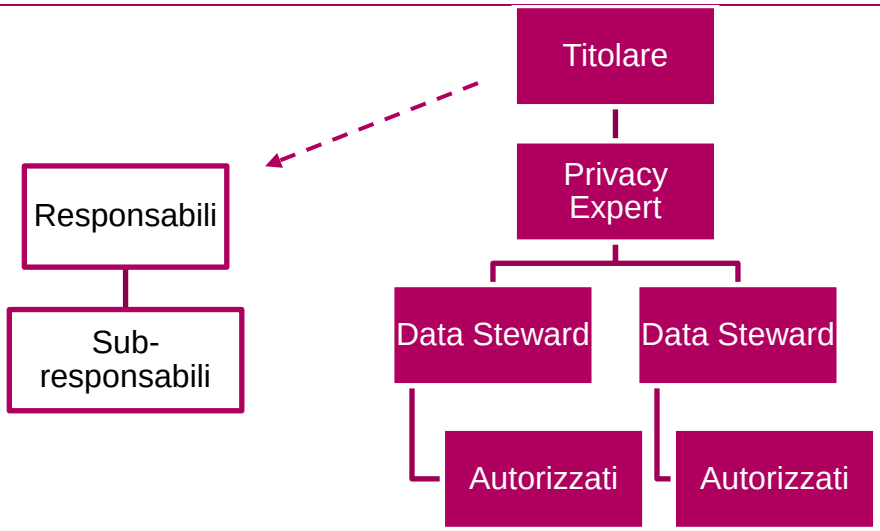
4 Ruoli e responsabilità

Il Modello Organizzativo di cui si è dotata la Società si articola su diversi livelli, riconoscendo poteri e relative responsabilità in capo a diversi soggetti:

- il titolare del trattamento è la Società, a cui spetta il compito di determinare le finalità e i mezzi del trattamento dei dati personali, nonché di adottare le misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali sia effettuato conformemente alla Normativa Privacy. In particolare, il Titolare è chiamato, a titolo esemplificativo e non esaustivo, a adottare le soluzioni di privacy by design e privacy by default; aggiornare il registro dei trattamenti; predisporre le informative relative al trattamento dei dati personali; predisporre ogni adempimento organizzativo necessario per garantire agli interessati l'esercizio dei diritti; disporre l'adozione dei provvedimenti imposti dall'Autorità di Controllo; effettuare la valutazione d'impatto ai sensi dell'Art. 35 GDPR; consultare l'Autorità di Controllo nei casi e secondo le modalità previste dall'Art. 36 GDPR; sottoscrivere con i responsabili del trattamento l'accordo previsto dall'Art. 28 GDPR;
- i responsabili del trattamento sono i soggetti terzi, esterni all'organizzazione della Società, che effettuano per conto e sotto le istruzioni del titolare le operazioni di trattamento dei dati di cui la Società è titolare; i responsabili del trattamento devono sottoscrivere con il titolare l'accordo di cui all'Art. 28 GDPR;
- i sub-responsabili del trattamento sono i soggetti terzi, esterni all'organizzazione della Società, ai quali il responsabile del trattamento affida lo svolgimento di determinate attività di trattamento mediante la sottoscrizione di un apposito accordo che impone al sub-responsabile gli stessi obblighi in materia di protezione dei dati contenuti nell'accordo sottoscritto con il titolare del trattamento di cui sopra;

- gli autorizzati al trattamento sono tutte le persone fisiche che effettuano operazioni di trattamento di dati personali su istruzione del titolare, ivi inclusi i dipendenti della Società che operano a qualsiasi titolo sotto la diretta autorità della Società;

- i Privacy Expert sono i soggetti individuati direttamente dalla Società che, nello svolgimento delle loro funzioni e nei limiti dei poteri attribuiti, fungono da punto di contatto per i Data Steward per le questioni in materia di trattamento di dati personali e, in particolare, le questioni relative al rispetto del presente Modello Organizzativo e della Normativa Privacy da parte della Società; i Privacy Expert sono raggiungibili all'indirizzo e-mail privacyexpert@falckrenewables.com
- i Data Steward sono i soggetti che, individuati dal responsabile dell'unità organizzativa di appartenenza, sono chiamati a supervisionare e a sovrintendere il rispetto del Modello Organizzativo da parte dei Destinatari, assistere la Società nell'attuazione delle Policy Privacy e agire come referenti principali per le questioni in materia di trattamento di dati personali all'interno della loro unità organizzativa, nonché fungere da punto di contatto per gli interessati e i Destinatari.



5 Principi applicabili al trattamento

I trattamenti effettuati dalla Società avvengono esclusivamente nel rispetto dei principi individuati dall'Art. 5 del GDPR ai sensi del quale i dati personali sono:

(a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;

(b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;

(c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;

(d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;

(e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;

(f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

A tal fine, i Destinatari sono tenuti ad accertare, prima di realizzare un trattamento di dati personali, il rispetto dei principi sopra indicati.

In caso di dubbi relativi alla corretta applicazione dei principi in relazione allo specifico trattamento i Destinatari possono rivolgersi al Data Steward.

6 Liceità del trattamento

I trattamenti effettuati dalla Società avvengono esclusivamente nel rispetto dei criteri di liceità individuati dall'Art. 6 del GDPR ai sensi del quale il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

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

(b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

(c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

(d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

(e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

(f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

A tal fine, i Destinatari sono tenuti ad accertare, prima di realizzare un trattamento di dati personali, la sussistenza di almeno uno dei requisiti di liceità sopra indicati.

In caso di dubbi relativi alla liceità del trattamento o in merito alla base giuridica da utilizzare in relazione allo specifico trattamento i Destinatari possono rivolgersi al Data Steward.

6.1 Il consenso

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. Il consenso deve essere:

- libero (l'interessato deve avere una scelta effettiva e il controllo sui propri dati, non deve sentirsi obbligato ad acconsentire o subire conseguenze negative se non acconsente);
- specifico (deve essere espresso in relazione a una o più specifiche finalità e l'interessato deve poter scegliere in relazione a ciascuna di esse);
- informato (fornire informazioni agli interessati prima di ottenerne il consenso è fondamentale per consentire loro di prendere decisioni informate, capire a cosa stanno acconsentendo e, ad esempio, esercitare il diritto di revocare il consenso);
- inequivocabile (richiede una dichiarazione o un'azione positiva inequivocabile da parte dell'interessato, il che significa che il consenso deve sempre essere espresso attraverso una dichiarazione o in modo attivo; non deve pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle).

L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento e 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.[2]

Alla luce di quanto sopra, i Destinatari sono tenuti ad accertare, prima di realizzare un trattamento di dati personali basato sul consenso, la sussistenza dei requisiti sopra indicati.

In caso di nuove operazioni di trattamento basate sul consenso, la redazione e/o aggiornamento dei formulari di consenso della Società spetta al Privacy Expert, con il supporto dei Data Steward e/o dei manager dell'unità organizzativa di riferimento. Resta inteso che il Privacy Expert, valutata la complessità dell'attività richiesta e previa comunicazione alla Società, potrà ricorrere al supporto di consulenti esterni per lo svolgimento dell'attività stessa.

Resta altresì inteso che i Destinatari non potranno, in nessun caso, modificare o aggiornare i formulari di consenso della Società senza la previa autorizzazione scritta del Privacy Expert. In caso di dubbi, i Destinatari possono rivolgersi al Data Steward.

6.2 Il legittimo interesse

Il legittimo interesse è uno dei sei criteri che legittimano il trattamento dei dati personali da parte del titolare. Di fatto, prevede che l'interesse legittimo del titolare del trattamento, oppure dei terzi cui vengono comunicati i dati, sia valutato rispetto agli interessi o ai diritti fondamentali dell'interessato. L'esito di questo test comparativo permette di stabilire se il legittimo interesse possa essere invocato come fondamento giuridico per il trattamento dei dati personali.

Per eseguire il test occorre valutare appieno una serie di fattori affinché sia possibile garantire che gli interessi e i diritti fondamentali degli interessati siano tenuti nella debita considerazione. Al tempo stesso, il test comparativo è adattabile, può variare da semplice a complesso e non deve risultare indebitamente gravoso. Tra i fattori di cui tenere conto nell'esecuzione del test comparativo figurano:

- la natura e l'origine dell'interesse legittimo, nonché l'eventualità che il trattamento dei dati sia necessario per l'esercizio di un diritto fondamentale o altrimenti per l'esecuzione di un compito di interesse pubblico o sia riconosciuto dalla comunità interessata;
- l'impatto sugli interessati e le loro ragionevoli aspettative su ciò che accadrà ai loro dati, nonché la natura dei dati e le modalità di trattamento;
- le garanzie supplementari che potrebbero limitare l'indebito impatto sull'interessato, quali la minimizzazione dei dati, le tecnologie di rafforzamento della tutela della vita privata, una maggiore trasparenza, il diritto generale e incondizionato di revoca e la portabilità dei dati.

Alla luce di quanto sopra, i Destinatari sono tenuti ad accertare, prima di realizzare un trattamento di dati personali basato sul legittimo interesse, che il titolare abbia svolto l'analisi di legittimo interesse sopra illustrata.

In caso di nuove operazioni di trattamento basate sul legittimo interesse, la redazione e/o aggiornamento dell'analisi di legittimo interesse della Società spetta al Privacy Expert, con il supporto dei Data Steward e/o dei manager dell'unità organizzativa di riferimento. Resta inteso che il Privacy Expert, valutata la complessità dell'attività richiesta e previa comunicazione alla Società, potrà ricorrere al supporto di consulenti esterni per lo svolgimento dell'attività stessa.

[2] Per ulteriori dettagli, si vedano anche le Guidelines on consent under Regulation 2016/679 dell'Article 29 Working Party.

Resta altresì inteso che i Destinatari non potranno, in nessun caso, modificare o aggiornare le analisi di legittimo interesse della Società senza la previa autorizzazione scritta del Privacy Expert. In caso di dubbi, i Destinatari possono rivolgersi al Data Steward.

7 Trasparenza

In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le informazioni previste dall'Art. 13 del GDPR. Infatti, devono essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che li riguardano nonché la misura in cui i dati personali sono o saranno trattati. Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro.

Il titolare comunica agli interessati le seguenti informazioni prima di realizzare un trattamento di dati personali:

(a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;

(b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;

(c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;

(d) i legittimi interessi perseguiti dal titolare del trattamento o da terzi, ove applicabile;

(e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;

(f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.

(g) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

(h) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;

(i) l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca, ove applicabile;

(j) il diritto di proporre reclamo a un'Autorità di Controllo;

(k) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;

(l) l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Alla luce di quanto sopra, i Destinatari sono tenuti ad accertare, prima di realizzare un trattamento di dati personali, che le informazioni di cui sopra siano correttamente fornite agli interessati attraverso le apposite informative predisposte dalla Società. In caso di dubbi, i Destinatari possono rivolgersi al Data Steward.

In caso di nuove operazioni di trattamento, la redazione e/o aggiornamento delle informative della Società spetta al Privacy Expert, con il supporto dei Data Steward e/o dei manager dell'unità organizzativa di riferimento. Resta inteso che il Privacy Expert, valutata la complessità dell'attività richiesta e previa comunicazione alla Società, potrà ricorrere al supporto di consulenti esterni per lo svolgimento dell'attività stessa.

Resta altresì inteso che i Destinatari non potranno, in nessun caso, modificare o aggiornare le informative della Società senza la previa autorizzazione scritta del Privacy Expert.

8 Conservazione

Uno dei principi generali stabiliti dal GDPR è che i dati personali devono essere 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. Al termine di tale periodo, i dati devono essere cancellati o anonimizzati in quanto non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati.[3]

Obblighi perentori di conservazione posso anche essere imposti da disposizioni normative, anche settoriali, o da obblighi contrattuali derivanti da accordi con fornitori di servizi o partner commerciali.

Al fine di garantire il rispetto del principio della limitazione della conservazione suddetto, la Società ha predisposto la policy sui tempi di conservazione di cui all'Allegato E, volta ad illustrare i tempi di conservazione che dovranno essere seguiti nelle attività di trattamento realizzate dai Destinatari.

Alla luce di quanto sopra, nell'ambito delle attività di trattamento da loro svolte, i Destinatari sono tenuti a verificare il puntuale rispetto dei tempi di conservazione suddetti. In caso di dubbi, i Destinatari possono rivolgersi al Data Steward.

9 Accordo con i responsabili del trattamento

Qualora un trattamento debba essere effettuato per conto della Società, quest'ultima 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 GDPR e garantisca la tutela dei diritti dell'interessato.

Inoltre, la Società sottoscrive con il responsabile un apposito contratto ai sensi dell'Art. 28 del GDPR che vincola il responsabile al titolare e che stipula 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.

Alla luce di quanto sopra, i Destinatari sono tenuti ad accertare, prima di realizzare un trattamento di dati personali che prevede il coinvolgimento di un responsabile del trattamento, che la Società abbia sottoscritto con lo stesso il contratto suddetto. In caso di dubbi, i Destinatari possono rivolgersi al Data Steward.

In caso di nuove operazioni di trattamento che prevedono il coinvolgimento di un responsabile del trattamento, la redazione e/o negoziazione del contratto suddetto spetta al Privacy Expert,

[3] Per rendere anonimi determinati dati, gli stessi devono essere privati di elementi sufficienti per impedire l'identificazione della persona interessata. Più precisamente, i dati devono essere trattati in maniera tale da non poter più essere utilizzati per identificare una persona fisica utilizzando "*l'insieme dei mezzi che possono essere ragionevolmente utilizzati*" dal titolare del trattamento o da altri e tale procedura deve essere irreversibile. Tra le tecniche di anonimizzazione più utilizzate vi sono le tecniche basate sulla randomizzazione, che modifica la veridicità dei dati al fine di eliminare la forte correlazione che esiste tra i dati e la persona (i.e. se i dati sono sufficientemente incerti non possono più essere riferiti a una persona specifica) e le tecniche basate sulla generalizzazione, che "diluisce" gli attributi delle persone interessate modificando la rispettiva scala o ordine di grandezza (vale a dire, una regione anziché una città, un mese anziché una settimana).

con il supporto dei Data Steward e/o manager dell'unità organizzativa di riferimento. Resta inteso che il Privacy Expert, valutata la complessità dell'attività richiesta e previa comunicazione alla Società, potrà ricorrere al supporto di consulenti esterni per lo svolgimento dell'attività stessa.

I Data Steward dovranno tenere l'elenco completo dei soggetti terzi nominati responsabili del trattamento e, ove possibile, degli eventuali sub-responsabili nell'ambito dell'unità organizzativa di appartenenza, nonché dare prontamente comunicazione di ogni aggiornamento e/o modifica dello stesso al Privacy Expert.

L'elenco completo dei responsabili del trattamento e, ove possibile, sub-responsabili della Società è disponibile presso il Privacy Expert.

10 Trasferimento dei dati personali verso Paesi Terzi

Qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo, compresi trasferimenti successivi di dati personali da un paese terzo verso un altro paese terzo, ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni previste dagli Art. 44 e seguenti del GDPR.

In particolare, il trasferimento di dati personali può avvenire solo qualora ricorra almeno una delle seguenti condizioni:

(a) il paese terzo ha ricevuto da parte della Commissione Europea una decisione di adeguatezza;[4]

(b) il titolare ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi (costituiscono garanzie adeguate, a titolo esemplificativo, le norme vincolanti d'impresa e le clausole tipo di protezione dei dati adottate dalla Commissione Europea).

Alla luce di quanto sopra, i Destinatari sono tenuti ad accertare, prima di realizzare un trattamento di dati personali che prevede il trasferimento di dati personali verso un paese terzo, la sussistenza di almeno uno dei requisiti sopra indicati. In caso di dubbi relativi al trasferimento dei dati personali verso Paesi Terzi, i Destinatari possono rivolgersi al Data Steward.

11 Diritti dell'interessato

Il GDPR consente all'interessato di esercitare in qualunque momento i seguenti diritti:

- diritto di accesso ai dati personali e alle seguenti informazioni: finalità del trattamento, categorie di dati personali in questione, destinatari o categorie di destinatari a cui i dati personali possono essere comunicati, il periodo di conservazione dei dati personali (ove possibile), nonché, qualora i dati personali non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
- diritto di rettifica dei dati personali inesatti;
- diritto di ottenere la cancellazione dei dati personali che la riguardano;
- diritto di richiedere la limitazione del trattamento;

[4] Le decisioni sinora adottate in materia di adeguatezza, in vigore fino a quando non vengano modificate, sostituite o abrogate dalla stessa Commissione Europea, sono elencate sul sito della Commissione Europea (https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en).

- diritto di ricevere o chiedere il trasferimento dei dati personali a lei riferibili in possesso del Titolare in un formato strutturato, di uso comune e leggibile, per ulteriori usi personali ovvero per fornirli ad altro titolare del trattamento;
- diritto di opporsi al trattamento;
- diritto di non essere sottoposto a una decisione basata unicamente su un trattamento automatizzato dei suoi dati personali, ove realizzato, che produca effetti giuridici che la riguardano o che incida in modo significativo sulla sua persona;
- diritto di revocare il consenso, anche per le finalità connesse all'invio delle comunicazioni commerciali (con effetto solo per il futuro);
- diritto di proporre reclamo all'Autorità di Controllo.

Ai diritti di cui sopra potrebbero applicarsi delle limitazioni qualora dall'esercizio degli stessi possa derivare un pregiudizio effettivo e concreto, ad esempio, agli interessi legittimi del titolare e, nonostante l'esercizio dei diritti sia di regola gratuito, il titolare può riservarsi il diritto di chiedere un contributo in caso di richieste manifestamente infondate o eccessive.

Il titolare del trattamento fornisce riscontro alla richiesta dell'interessato senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Resta inteso che, in caso di proroga, il titolare del trattamento informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta.

I Destinatari sono tenuti ad assistere la Società al fine di consentire alla stessa la corretta gestione delle richieste presentate dagli interessati e, nel caso di richieste da parte degli interessati, a comunicarle senza ingiustificato ritardo al Data Steward che provvederà a comunicarle al Privacy Expert, in modo che sia possibile dare riscontro agli interessati entro i termini perentori sopra indicati.

12 Violazione dei dati personali

Il GDPR prevede che il titolare, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, debba notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Infatti, una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Si elencano di seguito alcuni esempi di violazione dei dati personali che dovranno essere comunicati tempestivamente al Data Steward:

- perdita di backup contenente dati personali;
- accesso a banche dati da parte di soggetti non autorizzati;
- attacco al sistema informatico;

- furto o smarrimento di computer, laptop, devices elettronici portatili, chiavette USB, smartphones/tablet della Società;
- furto di identità e/o *phishing*.

Al fine di garantire la corretta gestione della violazione dei dati personali, la limitazione degli effetti pregiudizievoli della stessa, nonché il rispetto degli obblighi di notifica suddetti, la Società ha predisposto la procedura per gestione della violazione dei dati personali di cui all'Allegato D, volta ad illustrare le modalità attraverso le quali la Società individua le azioni necessarie da implementare nei casi in cui vi sia una reale o sospetta violazione dei dati personali. Detta procedura individua altresì i soggetti deputati alla valutazione della gravità della violazione dei dati personali.

A tal fine, i Destinatari sono tenuti, in conformità con quanto previsto dalla procedura suddetta, a segnalare ogni potenziale violazione dei dati di cui possano venire a conoscenza, contattando tempestivamente il Data Steward, nonché ad assistere la Società al fine di consentire la corretta gestione della violazione dei dati personali.

13 Registro delle attività di trattamento

Il titolare del trattamento è obbligato a tenere un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni previste dall'Art. 30 del GDPR:

(a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;

(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 e 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 implementate.

Alla luce di quanto sopra, la Società ha provveduto ad implementare il registro dei trattamenti al fine di mappare le diverse operazioni di trattamento dei dati personali effettuate sotto la sua responsabilità, effettuare una corretta analisi del rischio e una corretta pianificazione dei trattamenti.

L'aggiornamento e l'integrazione del registro dei trattamenti è affidato dalla Società al Privacy Expert che, con cadenza almeno semestrale, effettua l'aggiornamento del registro sulla base delle comunicazioni di aggiornamento fornite, con cadenza almeno trimestrale, dai Data Steward, con riferimento all'unità organizzativa di appartenenza.

14 Valutazione di impatto

Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una

valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.[5]

Si tratta di uno degli elementi di maggiore rilevanza nel nuovo quadro normativo, perché esprime chiaramente la responsabilizzazione del titolare nei confronti dei trattamenti effettuati.

La valutazione di impatto è obbligatoria in tutti i casi in cui un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Tra i casi in cui potrebbe essere necessaria la valutazione di impatto vi sono i seguenti:

- trattamenti valutativi o di scoring, compresa la profilazione;
- decisioni automatizzate che producono significativi effetti giuridici (ad esempio: assunzioni);
- monitoraggio sistematico (ad esempio: videosorveglianza);
- trattamento di dati sensibili, giudiziari o di natura estremamente personale (ad esempio: informazioni sulle opinioni politiche);
- trattamenti di dati personali su larga scala;
- combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data);
- dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani);
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (ad esempio: riconoscimento facciale, device IoT);
- trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

La valutazione di impatto contiene almeno:

(a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

(b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

(c) una valutazione dei rischi per i diritti e le libertà degli interessati;

(d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

La valutazione di impatto deve essere condotta prima di procedere al trattamento e dovrebbe comunque essere previsto un riesame continuo della valutazione, ripetendo la valutazione a intervalli regolari.

In questo senso, la valutazione di impatto permette di rispettare concretamente i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default di cui all'Art. 25 del GDPR di qualsiasi trattamento. Infatti, il titolare, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, mette in atto misure tecniche e organizzative adeguate, volte ad attuare in modo efficace i principi di protezione dei dati e a

[5] Per ulteriori dettagli, si vedano anche le Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 dell'Article 29 Working Party.

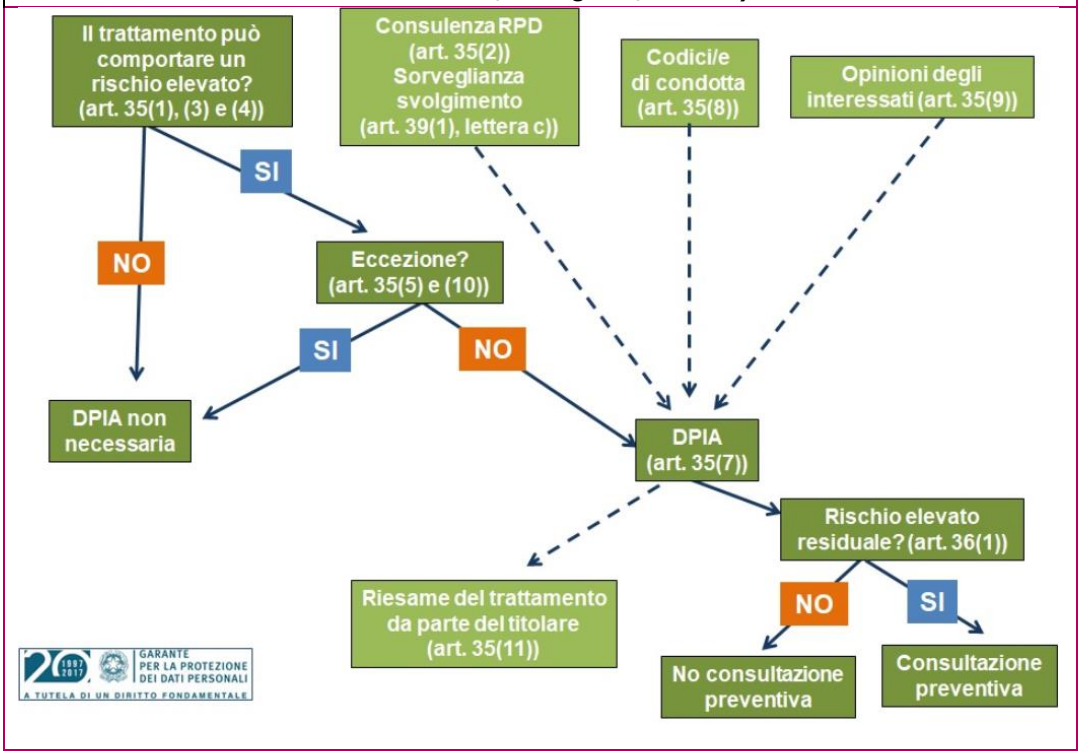
integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del GDPR e tutelare i diritti degli interessati (principio di privacy-by-design).

Allo stesso modo, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento (principio di privacy-by-default).

Alla luce di quanto sopra e al fine di garantire il corretto svolgimento della valutazione di impatto, nonché il rispetto dei principi di privacy-by-design e di privacy-by-default suddetti, la Società ha predisposto il documento di cui all'Allegato B. Lo stesso dovrà essere inteso come un supporto, da adattare alle peculiarità del caso specifico, per lo svolgimento della valutazione di impatto.

La Società ha affidato al Privacy Expert le attività relative allo svolgimento della valutazione di impatto, ivi inclusa la preventiva fase di scelta sulla necessità di procedere alla stessa, che dovranno essere svolte d'intesa con il Data Steward e/o manager dell'unità organizzativa di riferimento, nonché dei Destinatari interessati. Il Privacy Expert dovrà quindi essere informato dal Data Steward e/o dal manager dell'unità organizzativa di riferimento di qualsiasi nuovo progetto. Il Privacy Expert, d'intesa con la società, tenuto conto della complessità della attività richiesta, potrà ricorrere al supporto di consulenti esterni per lo svolgimento dell'attività stessa.

Quando effettuare la valutazione d'impatto (in inglese *Data Protection Impact Assessment* e, di seguito, "DPIA")?



15 Monitoraggio e controllo

Al fine di verificare il rispetto del presente Modello Organizzativo e della Normativa Privacy da parte dei Destinatari, inclusi i responsabili del trattamento, la Società effettua, con cadenza almeno annuale, il monitoraggio e il controllo dei trattamenti realizzati dalla Società e del rispetto, da parte Destinatari, del Modello Organizzativo.

Alla luce di quanto sopra, la Società ha affidato le attività di monitoraggio e controllo sopra descritte al Privacy Expert.

A seguito di tali controlli, il Privacy Expert invierà, con cadenza almeno annuale all'amministratore delegato della Società e, per conoscenza, all'Internal Audit, un report indicante, tra le altre, eventuali richieste ricevute dell'Autorità di Controllo, eventuali inosservanze rilevate in materia di protezione dei dati personali ed i relativi correttivi, i rischi o problematiche rilevanti connesse al trattamento dei dati personali, un elenco delle valutazioni di impatto svolte e/o suggerite, nuovi progetti e la conformità degli stessi ai principi di privacy by design e by default.

16 Formazione

Per un efficace funzionamento del Modello Organizzativo, la formazione dei Destinatari autorizzati al trattamento è gestita dalla Società in stretta cooperazione con il Privacy Expert e il dipartimento risorse umane della Società. In particolare, i corsi di formazione hanno ad oggetto l'intero Modello Organizzativo in tutte le sue componenti nonché le nozioni relative alla Normativa Privacy.

La partecipazione ai corsi di formazione è monitorata attraverso un sistema di rilevazione delle presenze. Al termine di ogni corso di formazione è sottoposto al partecipante un test finalizzato a valutare il grado di apprendimento conseguito e ad orientare ulteriori interventi formativi. La partecipazione ai corsi di formazione è obbligatoria per tutti i Destinatari autorizzati al trattamento dalla Società. Tale obbligo costituisce una regola fondamentale del presente Modello Organizzativo, alla cui violazione sono connesse le sanzioni previste nel sistema disciplinare.

I Destinatari della formazione sono tenuti a:

- acquisire conoscenza dei principi e dei contenuti del Modello Organizzativo;
- conoscere le modalità operative con le quali deve essere realizzata la propria attività;
- contribuire attivamente, in relazione al proprio ruolo e alle proprie responsabilità, all'efficace attuazione del Modello Organizzativo, segnalando eventuali carenze riscontrate nello stesso.

17 Inosservanza del Modello Organizzativo

Si porta a conoscenza di tutti i Destinatari che il presente Modello Organizzativo, nonché le Policy Privacy che ne formano parte integrante e sostanziale, ha carattere vincolante per i Destinatari.

Eventuali violazioni del Modello Organizzativo, nonché delle Policy Privacy, possono avere gravi ripercussioni sulla Società e comportare, nei confronti dei Destinatari dipendenti della Società inadempienti, l'applicazione di provvedimenti disciplinari, in conformità alle disposizioni di legge e del contratto collettivo nazionale applicabile e, nei confronti dei Destinatari non dipendenti della Società, la cessazione del rapporto contrattuale con la Società, fatta salva ogni ulteriore azione a tutela di ogni diritto della Società.

I comportamenti che costituiscono violazione del presente Modello Organizzativo possono determinare, allo stesso tempo, la violazione di disposizioni di legge tali da implicare per i Destinatari inadempienti conseguenze di natura civile e penale.

Anche la Società può essere perseguita e sanzionata in conseguenza della condotta inadempiente dei Destinatari e la violazione delle disposizioni previste dal GDPR può comportare l'applicazione di sanzioni amministrative pecuniarie fino a 20.000.000 EURO o fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

18 Aggiornamenti e modifiche

Il presente Modello Organizzativo può essere aggiornato, modificato o integrato in ogni momento dalla Società. In tale evenienza, le modifiche saranno portate all'attenzione dei Destinatari nel più breve tempo possibile attraverso la pubblicazione sui canali informativi della Società. A tal fine, i Destinatari sono tenuti

a consultare periodicamente i canali di comunicazione interni e prendere visione della versione aggiornata del Modello Organizzativo.

19 Contatti

In caso di quesiti o dubbi in merito al presente Modello Organizzativo o alle Policy Privacy si prega di contattare il Privacy Expert al seguente indirizzo e-mail: privacyexpert@falckrenewables.com.

20 Elenco allegati

A. Policy sull'utilizzo degli strumenti informatici (16)

B. Valutazione di impatto sulla protezione dei dati (24)

C. F.A.Q. (31)

D. Data Breach Policy (**Errore. Il segnalibro non è definito.**)

E. Data Retention Policy (45)

Allegato A
Policy sull'utilizzo degli strumenti informatici

1 Ambito di applicazione

Lo scopo della presente policy è definire le regole e le modalità con cui i dipendenti, collaboratori e consulenti della Società ("**Utenti**") possono utilizzare il personal computer, il tablet, lo smartphone, le loro periferiche (incluse *web-cam*, microfoni e periferiche audio) e qualsiasi altro strumento informatico loro assegnato o messo a disposizione dalla Società ("**strumenti informatici**") per svolgere le loro mansioni.

Alla presente policy si applicano le definizioni del Modello Organizzativo. Resta inteso che ogni riferimento alla Società contenuto all'interno della presente policy dovrà essere inteso come rivolto a ciascuna società del Gruppo.

2 Utilizzo degli strumenti informatici

Gli strumenti informatici costituiscono strumento di lavoro.

L'utilizzo è consentito esclusivamente per finalità direttamente attinenti o comunque connesse con l'attività lavorativa, secondo criteri di correttezza e professionalità, coerentemente al tipo di attività svolta ed in linea con le disposizioni di legge e le policy della Società, comunque con esclusione di qualsivoglia uso per scopi privati e/o personali.

Gli strumenti informatici sono affidati dalla Società agli Utenti, con ogni conseguente obbligo di custodia e di utilizzo appropriato. Gli Utenti devono utilizzare gli strumenti informatici con la massima attenzione e diligenza.

Alla data di cessazione del rapporto contrattuale con la Società, l'Utente dovrà restituire gli strumenti informatici alla Società.

L'utilizzo degli strumenti informatici non configura alcuna titolarità, da parte dell'Utente autorizzato, dei dati o delle informazioni trattate per il tramite di detti strumenti informatici, che appartengono unicamente alla Società e che si riserva pertanto, nei limiti consentiti dalle disposizioni di legge, il diritto di accedervi, con le modalità di seguito illustrate.

L'utilizzo degli strumenti informatici della Società non conforme alla presente policy, o comunque contrario alla legge, può dar luogo all'applicazione di sanzioni disciplinari, ivi incluso il licenziamento.

2.1 Obblighi

Gli Utenti devono:

- spegnere gli strumenti informatici ed eventuali periferiche (ad esempio: personal computer e monitor) al termine dell'attività lavorativa o in caso di allontanamenti protratti dal posto di lavoro, in assenza di ulteriori indicazioni da parte degli amministratori di sistema;
- adottare le altre cautele previste dalle procedure e/o istruzioni fornite dalla Società, anche in caso di brevi allontanamenti;
- far eseguire le operazioni di manutenzione e/o riparazione degli strumenti informatici solo da parte del personale autorizzato della Società;
- evitare qualsiasi uso di strumenti informatici personali sul luogo di lavoro o per usi lavorativi, salvo che ciò sia stato espressamente autorizzato dalla Società;
- con regolare periodicità (almeno ogni tre mesi), provvedere alla pulizia degli archivi (cartelle di dati e casella di posta elettronica), con cancellazione dei file obsoleti o inutili;

- segnalare tempestivamente ogni anomalia o malfunzionamento, anche parziale, degli strumenti informatici, nonché informare immediatamente la Società nell'ipotesi di furto o danneggiamento degli stessi;
- rispettare le ulteriori policy, istruzioni e/o procedure fornite dalla Società e relative all'utilizzo degli strumenti informatici.

2.2 Divieti

Gli Utenti non devono:

- installare sugli strumenti informatici software, anche se gratuiti (freeware o shareware), non distribuiti e/o comunque non espressamente autorizzati dalla Società, né collegare agli strumenti informatici periferiche hardware o dispositivi non messi a disposizione dalla Società;
- modificare le impostazioni di sicurezza e di riservatezza del sistema operativo, del software di navigazione, del software di posta elettronica, e di ogni altro software installato sugli strumenti informatici;
- modificare o disattivare in alcun modo la funzione di screen saver con password della propria posizione di lavoro;
- caricare o comunque detenere all'interno degli strumenti informatici materiale informatico, dati ed informazioni personali o comunque di contenuto non attinente alla mansione ricoperta;
- caricare o comunque detenere materiale informatico il cui contenuto (ad esempio: testo, audio o video) sia coperto da diritto d'autore, attenga o riguardi dati confidenziali (salvo che si tratti di dati che è indispensabile trattare con tali mezzi, conformemente alle disposizioni ed istruzioni, per le mansioni attribuite), consenta di conoscere dati confidenziali, sia contrario a norme di legge e/o comunque concerna attività ludiche o di svago;
- condurre attività che diminuiscano la performance dei sistemi e servizi della Società, li rendano indisponibili o introducano delle vulnerabilità o minacce alla sicurezza.

Tutta la gestione degli strumenti informatici, incluse le modifiche alla configurazione del sistema, può essere effettuata unicamente dalla Società o da soggetti espressamente autorizzati dalla Società. Ad esempio, sono considerate modifiche del sistema e, pertanto, non possono essere compiute se non previa autorizzazione della Società:

- la modifica dei collegamenti di rete esistenti;
- l'utilizzo dei dispositivi removibili (ad esempio: USB, CD, DVD, hard disk);
- l'apertura della struttura esterna (*case*) degli strumenti informatici e la modifica, eliminazione o aggiunta di componenti degli stessi;
- l'installazione di un qualsiasi software, inclusi quelli scaricati da Internet, o comunque di alterazione della configurazione degli strumenti informatici ricevuta in assegnazione.

Il personale incaricato dalla Società può in qualunque momento procedere alla rimozione di file o applicazioni che ritiene essere pericolosi per la sicurezza della Società sia sugli strumenti informatici sia sulle unità di rete.

3 Gestione delle password

L'accesso agli strumenti informatici è condizionato al corretto inserimento delle credenziali di autenticazione (nome utente e password).

È necessario scegliere la password rispettando le seguenti regole:

- utilizzando almeno otto caratteri, almeno un carattere numerico, almeno un carattere alfabetico maiuscolo e almeno uno minuscolo, almeno un carattere speciale;
- una password non deve essere una parola del dizionario, una parola dialettale o gergale di qualsiasi lingua, o una qualsiasi di queste parole scritte al contrario;
- le password non devono essere basate su dati personali dell'Utente o di un familiare (ad esempio: data di nascita, indirizzo, nome);
- non può essere uguale alle ultime dieci utilizzate.

Gli Utenti devono applicare le seguenti regole sicurezza quando selezionano e usano le password:

- le password non devono essere divulgate ad altre persone, inclusi gli amministratori di gestione e di sistema;
- le password non devono essere trascritte, a meno che un metodo sicuro sia stato approvato dalla Società;
- le password generate dall'Utente non devono essere distribuite attraverso alcun canale;
- le password devono essere cambiate se vi sono indicazioni che le password o il sistema possano essere stati compromessi (in tal caso deve essere segnalato un incidente di sicurezza alla Società).

Quando si assegnano o si utilizzano password devono essere rispettate le seguenti regole:

- gli Utenti hanno l'obbligo di mantenere riservate le password e non possono condividere il proprio nome utente con altri Utenti;
- ciascun Utente deve avere la possibilità di scegliere la propria password, laddove applicabile;
- la password temporanea utilizzata per il primo accesso al sistema deve essere unica e deve rispettare le regole di cui sopra;
- il sistema di gestione delle password deve richiedere all'Utente di modificare la password temporanea al primo accesso al sistema;
- le password temporanee devono essere comunicate all'Utente in modo sicuro e l'identità dell'utente deve essere controllata preventivamente;
- il sistema di gestione delle password deve richiedere all'Utente di selezionare password complesse;
- il sistema di gestione delle password deve richiedere agli Utenti di cambiare le loro password ogni trenta giorni;
- la password non deve essere visibile sullo schermo durante l'accesso;
- se un Utente immette una password errata per 10 volte consecutive, il sistema deve bloccare l'account in questione.

4 Posta elettronica

4.1 Finalità di utilizzo

La Società mette a disposizione degli Utenti il servizio di posta elettronica, assegnando a ciascuno di essi caselle di posta istituzionali per fini esclusivamente lavorativi.

L'indirizzo di posta elettronica messo a disposizione degli Utenti dalla Società costituisce esclusivamente uno strumento di lavoro. Pertanto, l'utilizzo della stessa da parte degli Utenti è consentito unicamente per

finalità direttamente attinenti o comunque connesse all'esercizio delle mansioni attribuite e alle attività di pertinenza, con esclusione di qualsivoglia uso per scopi o motivi privati e/o personali.

Al fine di agevolare lo svolgimento dell'attività lavorativa, la Società può rendere, inoltre, disponibili indirizzi di posta elettronica condivisi tra più Utenti (ad esempio: caselle di posta istituite per singole unità organizzative), affiancandoli a quelli individuali.

4.2 Divieti

Al fine di un corretto utilizzo della posta elettronica è vietato:

- utilizzare la posta elettronica per scopi personali e comunque per inviare o ricevere software o materiale informatico o dati o informazioni di qualsiasi tipo per scopi personali, ad esempio per la partecipazione o iscrizione a dibattiti, aste online, concorsi, forum, social network o mailing-list, salvo che ciò sia stato espressamente autorizzato dalla Società o sia necessario per lo svolgimento delle proprie mansioni lavorative;
- l'invio o lo scambio e l'archiviazione di messaggi di posta elettronica contenenti dati personali sensibili o giudiziari o idonei a rivelare dati sensibili o giudiziari (salvo che ciò sia necessario per l'espletamento delle proprie mansioni);
- partecipare a catene telematiche (o di Sant'Antonio); se dovessero peraltro essere ricevuti messaggi di tale tipo si dovrà procedere alla loro immediata eliminazione;
- l'invio o la memorizzazione di messaggi di natura oltraggiosa, volgare, diffamatoria e/o discriminatoria per sesso, razza, lingua, religione, origine etnica, opinione ed appartenenza sindacale e/o politica, contrari a norme di legge, alla decenza o al pudore, o comunque di contenuto oltraggioso o in ogni altro modo idonei ad offendere o vessare, nonché di messaggi a catena e/o spam;
- l'uso di linguaggio o di immagini oscene, ingannevoli, diffamatorie, discriminatorie e/o comunque suscettibili di creare un danno alla Società o a terzi;
- lo scambio di messaggi sotto mentite spoglie, ossia impersonando un mittente diverso da quello reale;
- inviare o ricevere o scambiare messaggi di posta, con o senza allegato, contenenti: immagini, filmati, e qualunque tipo di file dai contenuti illegali, violenti e/o pornografici; file soggetti al diritto d'autore (ad esempio: file musicali o video); link a siti con contenuti illegali, violenti e/o pornografici; password e/o codici di accesso a programmi soggetti a diritto d'autore e/o a siti internet;
- aprire messaggi di posta o allegati di tipo "eseguibile" (ad esempio: *.exe*) o che facciano riferimenti a link esterni.

4.3 Obblighi

Gli Utenti devono:

- limitare la dimensione dei messaggi inviati, soprattutto nei casi in cui vi siano più destinatari;
- evitare ogni comportamento che possa consentire a terzi di divulgare informazioni di qualsiasi tipo riconducibili ad un mittente inconsapevole;
- evitare di rispondere a messaggi di posta che contengono un messaggio generico di richiesta di informazioni personali per motivi non chiaramente specificati (ad esempio: scadenza, smarrimento, problemi tecnici) o che fanno uso di toni intimidatori (ad esempio: la minaccia del blocco della carta di credito o del conto corrente) o comunque caratterizzati da elementi che possano rivelare azioni di *phishing*;

- mantenere in ordine la casella di posta elettronica, eliminando i messaggi non necessari e archiviando nelle apposite sezioni i messaggi importanti per la Società, contenendo la dimensione degli stessi e dei relativi allegati, cancellando, pertanto, documenti inutili e soprattutto allegati ingombranti; resta inteso che la distruzione di ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per la Società ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura o comunque avente per altre ragioni tale contenuto deve essere autorizzata per iscritto dalla Società.

4.4 Assenza dell'Utente

In caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, l'Utente potrà:

(i) inserire autonomamente nel sistema una "risposta automatica" che avvisi i mittenti dei messaggi a lui indirizzati della sua assenza e suggerisca loro un destinatario alternativo con indirizzo di posta nel dominio @falckrenewablesgroup.com o @vectrorenewables.com

(ii) previa approvazione scritta del Data Steward della propria struttura, richiedere che i messaggi a lui indirizzati siano inoltrati automaticamente ad un altro destinatario con indirizzo di posta nel dominio @falckrenewablesgroup.com o @vectorenewables.com;

(iii) previa approvazione del Data Steward della propria struttura, delegare un altro Utente (fiduciario) a verificare il contenuto di messaggi e a inoltrare alla Società quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa; in questo caso l'amministratore del sistema di posta elettronica redigerà un verbale dell'attività e informerà l'Utente dell'accesso effettuato alla prima occasione utile.

Nel caso in cui l'Utente si trovi nella condizione di non poter effettuare le richieste di cui sopra (ad esempio: ricovero ospedaliero con limitate capacità psico-fisiche), la Società, per il tramite dell'amministratore di sistema e previa approvazione scritta del Privacy Expert, procederà implementando la soluzione (i) e, qualora vi siano specifiche e motivate esigenze di continuità del business che rischiano di essere impattate dall'assenza improvvisa e prolungata del dipendente, potrà accedere al contenuto della casella di posta elettronica. In questo caso, l'amministratore del sistema di posta elettronica redigerà un verbale dell'attività e informerà l'Utente dell'accesso effettuato alla prima occasione utile.

4.5 Firma

La corrispondenza elettronica in uscita deve sempre contenere a piè di pagina il seguente disclaimer sulla riservatezza della comunicazione:

"Questo messaggio può contenere informazioni di carattere estremamente riservato e confidenziale. Qualora non foste i destinatari, vi preghiamo di notificarcelo e di provvedere ad eliminare il messaggio, con gli eventuali allegati, senza trattenerne copia. Qualsivoglia utilizzo, integrale o parziale, non espressamente autorizzato del presente messaggio da parte del destinatario (quale, a titolo meramente esemplificativo e non limitativo, la pubblicazione o riproduzione su Internet o la distribuzione e/o diffusione a terzi in genere) espone il responsabile alle relative conseguenze civili e penali. Rispetta l'ambiente. Non stampare questa mail se non è strettamente necessario.

This message may contain information which is confidential or privileged. If you are not the intended recipient, please immediately notify us and destroy this message and any attachments without retaining a copy. Any unauthorized use of this message either whole or partial (including, without limitation, any copying or reproduction on internet websites and any distribution and/or diffusion to third parties) may expose the responsible party to civil and/or criminal penalties. Respect nature. Do not print this e-mail unless absolutely necessary."

5 Internet

L’accesso ad Internet è permesso agli Utenti autorizzati dalla Società unicamente per lo svolgimento delle proprie attività lavorative e sempre nel rispetto delle procedure interne e delle leggi applicabili.

Resta inteso che è severamente vietato:

- modificare le impostazioni dei sistemi al fine di evitare qualsiasi protezione volta a limitare l'accesso a Internet;
- stabilire, per qualsiasi motivo, connessioni peer-to-peer a Internet;
- scaricare file di grandi dimensioni, al fine di evitare la saturazione della larghezza di banda di rete disponibile per i sistemi;
- scaricare software, anche gratuiti (freeware e shareware), non aderenti agli standard della Società, onde evitare illeciti e soprattutto il grave pericolo di introdurre virus informatici.

6 *Smart-working*

Nel caso di utilizzo di strumenti informatici da parte degli Utenti durante l’esecuzione del rapporto di lavoro, definita mediante accordo tra la Società e gli Utenti, anche con forme di organizzazione per fasi, cicli e obiettivi e senza precisi vincoli di orario o di luogo di lavoro (“***smart-working***”), si applicano tutte le regole illustrate dalla presente policy.

È necessario che l’Utente sia autorizzato dalla Società per poter utilizzare strumenti informatici propri durante lo *smart-working*. In questo caso, l’Utente:

- deve utilizzare esclusivamente sistemi e software di cui è in possesso di regolare licenza di utilizzo e rispettare i termini e condizioni di utilizzo previsti dalla licenza;
- verificare che il sistema utilizzato sia regolarmente aggiornato sia per la parte di software di base che per i sistemi antivirus e antispam installati;
- verificare che la rete internet (anche *Wi-Fi*) utilizzata sia protetta da password per garantire che sia improbabile l’accesso da parte di persone non autorizzate alla rete stessa;
- garantire il rispetto delle regole e dei principi di sicurezza illustrati dalla presente policy.

7 Controllo e monitoraggio

Per ragioni organizzative e produttive, per la tutela del patrimonio aziendale e per verificare il rispetto delle leggi e normative applicabili, ivi incluse le policy aziendali della Società, la Società può avere la necessità di controllare l’utilizzo dei propri sistemi informatici e, ad esempio, accedere alle e-mail inviate o ricevute dall’Utente. Tale attività non è tuttavia da considerarsi quale attività di monitoraggio dell’attività del dipendente ed è condotta in conformità alle disposizioni di legge previste in materia di diritti dei lavoratori ed alla Normativa Privacy.

Le attività di controllo per i motivi predetti sono svolte, nel rispetto della privacy degli Utenti, dal personale della società che presta la propria attività per la gestione e l’assistenza dei servizi informativi aziendali in qualità di responsabile del trattamento dei dati personali con il supporto, ove necessario, del responsabile dell’unità organizzativa interessata, che individuerà l’oggetto della ricerca non potendo la stessa essere indiscriminata, generica e illimitata. Nessun altro soggetto sarà coinvolto in tali attività, né accederà ai dati personali degli Utenti contenuti negli account di posta elettronica aziendali

La Società ricorda agli Utenti che, poiché i sistemi informatici della Società sono dotati di sistemi di registrazione tecnica degli eventi occorsi (i.e. file di *log*), la Società potrà accedere a tali dati per le finalità di controllo suddette. Tali registrazioni potranno essere utilizzate per cercare la fonte di possibili errori o anomalie ma non possono essere utilizzate per tracciare l’attività lavorativa degli Utenti.

Le ragioni per cui la Società potrebbe effettuare una attività di controllo includono:

- identificare e prevenire qualsiasi accesso o comunicazione di informazioni non autorizzati;
- assicurare conformità alle leggi e ai regolamenti;
- prevenire, identificare o reprimere un'attività criminale;
- controllare i virus e altre minacce di codice malevolo;
- ove vi sia un sospetto, investigare o identificare usi inappropriati degli strumenti informatici;
- ove vi sia un sospetto, investigare violazioni della presente o di altre policy specifiche della Società.

Il monitoraggio viene effettuato nei limiti di quanto permesso o richiesto dalla legge e in quanto necessario e giustificabile per gli scopi sopra illustrati.

Le informazioni identificate durante il monitoraggio (compresi i dati personali) possono essere utilizzate anche per finalità disciplinari e conservate per la durata di ogni procedimento investigativo, disciplinare, regolamentare o criminale e possono essere comunicate a terze parti quando necessario o richiesto dalla legge.

Gli Utenti possono contattare il Privacy Expert per ulteriori informazioni sull'ambito e il tipo di controllo eventualmente effettuato sui sistemi informatici della Società.

8 Utilizzo dei social media

L'accesso ai propri account personali di social media quali, ad esempio, Facebook, Twitter, Instagram, non è consentito utilizzando gli strumenti informatici della Società.

Resta inteso che l'utilizzo dei propri account personali sui social media quali, ad esempio, Facebook, Twitter, Instagram, al di fuori dell'orario di lavoro e utilizzando strumenti informatici propri dovrà essere effettuato senza arrecare pregiudizio alla Società (ad esempio, non è possibile pubblicare documenti riservati della Società). A tal fine, la Società precisa che:

- qualsiasi uso che violi le leggi e i regolamenti applicabili, l'ordine pubblico, qualsiasi regola di decenza e/o che potrebbe danneggiare la reputazione e l'immagine della Società all'interno e all'esterno è severamente vietato;
- qualsiasi discussione o pubblicazione su social media sui prodotti, progetti o servizi della Società è consentita solo agli Utenti espressamente autorizzati;
- è vietato condividere informazioni su performance, progetti, prodotti, servizi, prospettive di sviluppo, dati finanziari, accordi commerciali, dati di vendita, strategie e risultati della Società nei social media a meno che gli Utenti non siano espressamente autorizzati;
- qualsiasi discussione o pubblicazione sui social media riguardante terzi competitor della Società e/o i loro prodotti o attività è vietata;
- prima di condividere qualsiasi contenuto protetto da diritti di proprietà intellettuale (ad esempio: nomi, marchi, loghi), ivi inclusi i diritti di cui la Società è titolare, è necessario ottenere un'autorizzazione specifica ed esplicita dal titolare dei diritti;
- i dati che consentono di identificare le persone e le loro relazioni professionali (ad esempio: clienti, fornitori, dipendenti, collaboratori) non devono essere pubblicati sui social media senza il consenso preventivo ed esplicito delle persone interessate;
- le idee e le opinioni devono essere espresse in modo rispettoso e appropriato secondo il contesto, al fine di evitare di danneggiare la dignità delle persone e/o delle imprese concorrenti.

Con riferimento all'utilizzo dei social media professionali e/o strettamente connessi all'attività lavorativa (i.e. Linkedin), gli Utenti devono inserire informazioni relative alla propria posizione aziendale e al ruolo ricoperto all'interno della Società veritiere, pertinenti e aggiornate.

Gli Utenti possono contattare il Data Stewart per ulteriori chiarimenti sull'utilizzo dei social media.

9 Riferimenti esterni.

- P_STAFF 30 GR – ITGov _ Gestione Accessi Logici
- P_STAFF 31 GR – ITSec _ Information Security Policy
- P_STAFF 27 GR – ITGov _ IT Tools Management Policy
- I_STAFF 18 GR – Op. Gestione Asset IT

Allegato B
Valutazione di impatto sulla protezione dei dati

1 Contesto

1.1 Panoramica del trattamento

1.1.1 Quale è il trattamento in considerazione?

1.1.2 Quali sono le responsabilità connesse al trattamento?

1.2 Dati, processi e risorse di supporto

1.2.1 Quali sono i dati trattati?

1.2.2 Quale è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

1.2.3 Quali sono le risorse di supporto ai dati?

2 Principi fondamentali

2.1 Proporzionalità e necessità

2.1.1 Gli scopi del trattamento sono specifici, espliciti e legittimi?

2.1.2 Quali sono le basi legali che rendono lecito il trattamento?

2.1.3 I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

2.1.4 I dati sono esatti e aggiornati?

2.1.5 Quale è il periodo di conservazione dei dati?

2.2 Misure a tutela dei diritti degli interessati

2.2.1 Come sono informati del trattamento gli interessati?

2.2.2 Come si ottiene il consenso degli interessati?

2.2.3 Come fanno gli interessati a esercitare i loro diritti ai sensi del Regolamento?

2.2.4 Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

2.2.5 In caso di trasferimento di dati al di fuori dell'Unione Europea, i dati godono di una protezione equivalente?

3 Rischi[6]

3.1 Misure esistenti o pianificate

No.	Nome del controllo	Descrizione	Controlli implementati
1.	Crittografia	I mezzi implementati per assicurare la confidenzialità dei dati archiviati (in database, file, backup, etc.), così come le procedure per gestire chiavi crittografiche (creazione, archiviazione, aggiornamento in caso di sospetta compromissione, etc.).	

[6] Il rischio non si riferisce al titolare ma al soggetto interessato.

		Specificare i mezzi crittografici impiegati per i flussi di dati (VPN, TLS, etc.) implementati nel trattamento.	
2.	Anonimizzazione	Indicare i meccanismi di anonimizzazione implementati, le garanzie da essi introdotti contro la eventuale re-identificazione e per quali finalità sono implementati.	
3.	Partizionamento	Metodi utilizzati per il partizionamento del trattamento.	
4.	Controllo degli accessi logici	Descrivere in che modo sono definiti e attribuiti i profili degli utenti. Specificare i mezzi di autenticazione implementati precisando, ove applicabili, le regole per le password (lunghezza minima, caratteri richiesti, durata della validità, numero di tentativi prima del blocco dell'account, etc.).	
5.	Tracciabilità	Politiche che definiscono la tracciabilità degli eventi e la gestione dei relativi log.	
6.	Archiviazione	Politiche di conservazione e gestione di archivi elettronici contenenti dati personali, finalizzate a tutelarne, in particolare, la validità giuridica per tutto il periodo necessario (versamento, conservazione, migrazione, accessibilità, eliminazione, politiche di archiviazione, protezione della confidenzialità, etc.).	
7.	Sicurezza dei documenti cartacei	Politiche relative ai documenti cartacei contenenti dati personali utilizzati nell'ambito del trattamento. Tali politiche descrivono come i documenti sono stampati, archiviati, distrutti e condivisi.	
8.	Minimizzazione della quantità di dati	Si possono utilizzare i seguenti metodi: filtraggio e rimozione, riduzione del potenziale identificativo attraverso trasformazione, riduzione della natura identificativa del dato, riduzione dell'accumulazione dei dati, limitazione dell'accesso ai dati.	
9.	Vulnerabilità	Politiche volte a limitare la probabilità e la gravità dei rischi per le risorse utilizzate durante l'operatività (documentare le procedure operative, inventario e aggiornamento di software e hardware, correzione di vulnerabilità, duplicazione dei dati, limitazioni all'accesso fisico al materiale, etc.).	
10.	Gestione postazioni	Misure adottate per ridurre la possibilità che le caratteristiche del software (sistemi operativi, applicazioni aziendali, software per ufficio, impostazioni etc.) vengano sfruttate per danneggiare i dati personali (aggiornamenti, protezione fisica e accesso, lavoro su uno spazio di rete protetto, controlli di integrità, *logging*, etc.).	
11.	Backup	Esistenza di politiche di backup tali da assicurare la disponibilità e/o l'integrità dei dati personali, tutelandone	

		la confidenzialità (periodicità dei backup, cifratura del canale di trasmissione dati, test di integrità, etc.).	
12.	Manutenzione	Esistenza di una politica di manutenzione fisica dei dispositivi, specificando l'eventuale ricorso all'outsourcing. Dovrà comprendere la manutenzione remota, ove autorizzata, e specificare i metodi di gestione dei materiali difettosi.	
13.	Accordi sul trattamento dati	I dati personali comunicati a o gestiti da responsabili del trattamento devono beneficiare di garanzie sufficienti. Utilizzare esclusivamente responsabili del trattamento che offrono garanzie sufficienti (in particolare quanto a conoscenze specialistiche, affidabilità e risorse). Esigere che il responsabile comunichi la propria politica di sicurezza dei sistemi informativi. Adottare e documentare misure (audit di sicurezza, visite agli impianti, etc.) che consentano di assicurare l'effettività delle garanzie offerte dal responsabile del trattamento in materia di protezione dei dati. Tali garanzie comprendono, in particolare: - la cifratura dei dati in base alla loro sensibilità ovvero, in assenza di cifratura, l'esistenza di procedure tali da garantire che il responsabile del trattamento non acceda ai dati affidatigli - la cifratura delle trasmissioni dei dati (p.es.: connessioni tipo HTTPS, VPN, etc.) - garanzie in materia di protezione della rete, tracciabilità (log, audit), gestione delle autorizzazioni, autenticazione, etc. Prevedere un contratto con i responsabili del trattamento, ove siano definiti, in particolare, oggetto, durata, finalità del trattamento e obblighi delle parti contraenti. Accertarsi che tale contratto contenga, in particolare, disposizioni relative a quanto segue: - gli obblighi dei responsabili in materia di riservatezza dei dati personali affidati - requisiti minimi di autenticazione degli utenti - clausole in materia di restituzione e/o distruzione dei dati allo scadere del contratto - regole per la gestione e la notifica di eventuali incidenti. Queste ultime dovrebbero prevedere la comunicazione al titolare del trattamento qualora sia individuata una violazione di sicurezza o si verifichi un incidente di sicurezza, da effettuarsi con la massima celerità possibile qualora la violazione riguardi dati personali.	

14.	Sicurezza dei canali informatici	A seconda del tipo di rete sulla quale il trattamento è effettuato (isolata, privata o internet), il titolare del trattamento deve implementare sistemi di protezione adeguati: firewall, sonde antintrusione o altri dispositivi (attivi o passivi) volti garantire la sicurezza della rete.	
15.	Controllo degli accessi fisici	Esistenza di un controllo degli accessi fisici ai locali che ospitano il trattamento (zonizzazione, accompagnamento di visitatori, assegnazione di badge, porte chiuse, e così via). Indicare se sono in atto procedure di allarme in caso di irruzione.	
16.	Tracciabilità delle attività della rete	Esistenza di misure messe in atto per rilevare tempestivamente incidenti relativi a dati personali e disporre di elementi utilizzabili per studiarli o per fornire prove nel contesto di indagini (politica di registrazione eventi, rispetto degli obblighi di protezione dei dati, etc.)	
17.	Sicurezza dell'hardware	Esistenza delle misure adottate per ridurre il rischio che le caratteristiche delle apparecchiature (server, postazioni fisse, portatili, periferiche, dispositivi di comunicazione, supporti rimovibili, etc.) siano utilizzate per danneggiare i dati personali (inventario, compartimentalizzazione, ridondanza, limiti per l'accesso, etc.)	
18.	Prevenzione delle fonti di rischio umane e non umane	Esistenza di misure per evitare che fonti di rischio, umane o non umane, anche se scarsamente probabili, arrechino pregiudizio ai dati personali (merci pericolose, aree geografiche pericolose, trasferimento dati al di fuori dell'UE, fenomeni climatici, incendio, danni provocati dall'acqua, incidenti interni o esterni, animali).	
19.	Politica di tutela della privacy	Esistenza di un'organizzazione idonea a guidare e verificare la protezione dei dati personali all'interno della struttura (designazione di un DPO/RPD, creazione di un organo di monitoraggio, etc.)	
20.	Gestione delle politiche di tutela della privacy	Il titolare del trattamento deve disporre di una base documentale che formalizzi gli obiettivi e le regole da applicare nel campo della protezione dei dati (piano d'azione, revisione periodica delle politiche in materia di protezione dati, etc.)	
21.	Gestione dei rischi	Esistenza di una politica che definisce i processi volti a controllare i rischi che i trattamenti comportano per i diritti e le libertà degli interessati (censimento dei trattamenti di dati personali, dei dati trattati, dei supporti utilizzati, valutazione del rischio, definizione di misure esistenti o previste, etc.)	
22.	Integrazione della protezione della	Esistenza di procedure che descrivono i metodi volti a tenere conto della protezione dei dati personali in ogni nuovo trattamento (certificazioni, specifiche di riferimento, gestione del rischio per la persona	

	privacy nei progetti	interessata secondo una metodologia interna o indicata dall'Autorità di Controllo, etc.)	
23.	Gestione degli incidenti di sicurezza e delle violazioni dei dati personali	Esistenza di un'organizzazione operativa per rilevare e gestire eventi che possono influire sulle libertà e sulla riservatezza degli interessati (definizione delle responsabilità, piano di reazione, caratterizzazione delle violazioni, etc.)	
24.	Gestione del personale	Esistenza di un piano che preveda le misure di sensibilizzazione adottate al momento della presa in carico di un dipendente e di una procedura che descrive le misure adottate una volta cessato il rapporto di lavoro con i soggetti che accedono ai dati.	
25.	Vigilanza sulla protezione dei dati	Esistenza di misure che consentano una visione globale e aggiornata dello stato di protezione dei dati e della conformità con il Regolamento (verifica della conformità dei trattamenti, obiettivi e indicatori, responsabilità, etc.).	
26.	Altri controlli		

3.2 Riservatezza dei dati (divulgazione/accesso)

3.2.1 Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?[7]

3.2.2 Quali sono le principali minacce che potrebbero concretizzare il rischio?

3.2.3 Quali sono le fonti di rischio?

3.2.4 Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

3.2.5 Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

3.2.6 Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

3.3 Integrità dei dati (alterazione)

3.3.1 Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

3.3.2 Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

3.3.3 Quali sono le fonti di rischio?

3.3.4 Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

3.3.5 Come stimereste la gravita del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?

3.3.6 Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?

3.4 Disponibilità dei dati (perdita/indisponibilità/distruzione)

[7] Ad esempio: furto d'identità, perdite finanziarie, danni fisici o psicologici, perdita di controllo dei dati, altri svantaggi economi o sociali, impossibilità di esercitare diritti/servizi/opportunità, danno per la reputazione, discriminazione.

3.4.1 Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

3.4.2 Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

3.4.3 Quali sono le fonti di rischio?

3.4.4 Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

3.4.5 Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

3.4.6 Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

3.5 Panoramica dei rischi con le misure correttive implementate[8]

	Riservatezza dei dati	**Integrità dei dati**	**Disponibilità dei dati**
Gravità			
Probabilità			
Risultato			

GRAVITÀ	Massimo 4	4	8	12	16
	Significativo 3	3	6	9	12
	Limitato 2	2	4	6	8
	Trascurabile 1	1	2	3	4
Livello di rischio (gravità per probabilità)		Trascurabile 1	Limitato 2	Significativo 3	Massimo 4
		PROBABILITÀ			

	TRASCURABILE	**LIMITATO**	**SIGNIFICATIVO**	**MASSIMO**
LIVELLO	L'interessato non sarà colpito o potrebbe incontrare pochi inconvenienti che potranno essere superati senza problemi.	L'interessato potrebbe incontrare significativi inconvenienti che potranno essere superati con qualche difficoltà.	L'interessato potrebbe subire significative conseguenze, che dovrebbe essere in grado di superare anche se con serie e reali difficoltà.	L'interessato potrebbe incontrare significative o irreversibili conseguenze che potrebbero non essere superabili.

4 Parere degli interessati

[•]

5 Indice delle versioni

[•]

6 Valutazioni conclusive

[8] Per ulteriori dettagli si prega di vedere le "Guidelines on Data Protection Impact Assessment (DPIA)" dell'Article 29 Working Party.

All’esito della valutazione di impatto, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio, nonché delle misure tecniche e organizzative adottate per attenuare l’eventuale rischio assicurando la protezione dei dati personali, la gravità del rischio risulta [●] e la probabilità del rischio risulta [●].

Allegato C
F.A.Q.

	Domanda	Risposta
1.	Il linguaggio dell'informativa privacy e della formula del consenso mi sembra di difficile comprensione, posso modificarlo?	No, solo il Privacy Expert può modificare questi documenti. Dovrai contattare il Data Steward della tua unità organizzativa che si consulterà con il Privacy Expert.
2.	Ci sono diverse formule di consenso, posso sostituirle con un'unica che comprenda tutto?	No, il consenso ai sensi del GDPR deve essere specifico. Ove quindi siano previsti più consensi questi dovranno essere separati. In ogni caso non è possibile sostituire le formule del consenso senza l'approvazione del Privacy Expert.
3.	Posso profilare i dipendenti o i clienti?	Ciò è possibile solo con riferimento agli individui che hanno prestato il consenso alla profilazione. In ogni caso, prima di intraprendere questa attività è necessario consultarsi con il Data Steward della propria unità organizzativa.
4.	Sto lavorando ad un nuovo prodotto o servizio che comporterà il trattamento di dati personali e prevedo di chiedere un parere dell'ufficio legale solo prima del lancio.	No, il GDPR richiede di valutare l'impatto sul trattamento dei dati di prodotti/servizi sin dall'inizio della progettazione secondo la procedura di cui al punto 12 della Data Protection Policy.
5.	Conservo nel cassetto della mia scrivania un elenco dei clienti "storici" contenente dati personali, lo posso fare?	No, esistono tempi di conservazione specifici per ciascuna tipologia di dato. Devi contattare il Data Steward perché la Società deve essere in grado di mappare tutti i trattamenti di dati personali detenuti per proprio conto.
6.	Sto per stipulare un contratto con un fornitore IT di cui mi fido perché ci lavoriamo da anni ed è molto famoso sul mercato. Posso evitare di effettuare i controlli in materia di conformità alla Normativa Privacy?	No, la procedura di cui al punto 8 della Data Protection Policy deve essere eseguita per ogni nuovo contratto stipulato dalla Società.
7.	Devo lavorare da casa durante il week-end, posso inviare i documenti sul mio indirizzo e-mail privato in modo da lavorarci con il mio computer personale?	No, ciò impedirebbe alla Società di proteggere il documento da un possibile accesso da parte di terzi. Non è possibile inviare documenti relativi all'attività lavorativa sulla propria e-mail privata e salvarli su dispositivi che non siano forniti dalla Società.
8.	Mi sono appena reso conto di aver dimenticato sul treno lo zaino con l'elenco dei clienti contenenti dati personali, che devo fare?	Devi contattare l'indirizzo e-mail databreach@falckrenewables.com in quanto esiste un rischio di accesso abusivo ai dati personali.
9.	Mi hanno rubato il computer aziendale, che cosa devo fare?	Devi contattare l'indirizzo e-mail databreach@falckrenewables.com in quanto esiste un rischio di accesso abusivo ai dati personali.

Allegato D
Data Breach Policy

Obiettivo della presente procedura (la "**Procedura**") è definire i principi, le modalità di individuazione, risoluzione ed i conseguenti flussi di gestione della Società in caso di violazione dei dati personali (**Data Breach**) ai sensi del Regolamento (UE) 2016/679 e della Normativa Privacy.

Sommario

1 Informazioni sul documento

1.1 Riferimenti normativi

- Regolamento (UE) 2016/679 del Parlamento e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito il "**Regolamento Privacy Europeo**" o "**GDPR**");
- Linee guida sul Data Breach del Gruppo di Lavoro di cui all'art. 29 della Direttiva 95/46/EC del 6 febbraio 2018 (di seguito "Gruppo ex art. 29").

1.2 Diffusione

Ogni Data Steward deve diffondere la presente procedura a tutti i componenti delle unità organizzative che agiscono sotto il suo coordinamento, sia in occasione della prima emissione sia in occasione di aggiornamenti che dovessero intercorrere successivamente alla prima emissione.

1.3 Destinatari della procedura

Tutti i dipendenti e collaboratori a tempo indeterminato o determinato della Società (di seguito congiuntamente definiti i "**Destinatari**").

1.4 Obbligo di conoscenza

I Destinatari hanno obbligo di conoscenza e rispetto dei contenuti della presente procedura.

1.5 Regole per l'approvazione, l'aggiornamento, l'archiviazione, la distribuzione della Procedura.

L'approvazione, l'aggiornamento e la modifica della presente procedura dovranno essere approvate dal Comitato Privacy in caso di aggiornamenti rilevanti, in accordo con le revisioni periodiche e le eventuali modifiche che potrebbero intervenire ai documenti del corpo normativo citati sopra, e comunque con cadenza annuale.

2 Definizioni

In aggiunta ai termini definiti nel documento di Data Protection Policy e ai termini definiti nel GDPR, i seguenti ulteriori termini hanno il significato di seguito indicato:

Comitato Privacy	Si intende il comitato formato dal Privacy Expert, dal **CDT&IO** e dal Data Steward della struttura di riferimento.
Data Breach o violazione dei dati personali	Si intende una 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.
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. Il dato personale può riferirsi solo ad una persona fisica (i.e. un individuo) e comprende anche ditte individuali e i liberi professionisti, mentre i dati delle persone giuridiche (i.e. società) non sono soggetti alla Normativa Privacy. Con riferimento all'indirizzo e-mail nome.cognome@falck.it è un dato personale, mentre l'indirizzo generico info@falck.it non è un dato personale.
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.
Privacy Expert	Il soggetto che agisce come contatto principale per ogni questione relativa alla conformità alla normativa privacy.
CDT&IO	Chief Digital Trasformation & Information Officer
Interessato	La persona fisica (ivi comprese le ditte crisis tendividuali e i liberi professionisti) identificabile direttamente o indirettamente tramite i dati personali oggetto del trattamento.
Autorità	Autorità di controllo competente
Crisis Team	Il Comitato consultivo, guidato dal *Gatekeeper*, preposto all'analisi dell'evento di crisi come definito nella Procedura di *Crisis Communication management*.

3 Scopo e ambito di applicazione della Procedura

Ai sensi dell'articolo 33 del GDPR in caso di violazione dei dati personali o Data Breach, il Titolare del Trattamento notifica la violazione all'autorità di controllo competente, , senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.
Ai sensi dell'articolo 34 del GDPR, inoltre, 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. Tale comunicazione non è richiesta ove:

- il Titolare del Trattamento abbia messo in atto le misure tecniche e organizzative adeguate di protezione dei dati personali e tali misure siano state applicate ai dati oggetto della violazione (e.g. cifratura);
- il Titolare del Trattamento abbia successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli Interessati;
- la comunicazione agli Interessati richieda sforzi sproporzionati (in tal caso il Titolare del Trattamento procederà ad una comunicazione pubblica o misura similare con analoga efficacia).

La presente procedura di Data Breach, redatta in conformità a quanto definito dal GDPR, viene attivata a fronte della rilevazione di una violazione di dati personali ed ha lo scopo di definire quali azioni devono essere intraprese dall'intera organizzazione aziendale in presenza di violazione dei principi sopra descritti. Nel presente documento trovano descrizione anche le circostanze, in presenza delle quali, viene ravvisato il bisogno di notificare e/o comunicare la violazione dei dati personali all'Autoritàe/o all'Interessato.
Il mancato rispetto delle regole riportate nel presente documento potrebbe comportare severe sanzioni.

La presente procedura ha l'obiettivo di:

- identificare le modalità e i canali di rilevazione di un Data Breach;
- prevedere un adeguato e tempestivo coinvolgimento delle Strutture aziendali apicali con riferimento agli eventi critici in materia di violazione dei dati personali al fine di garantire un'azione immediata in conformità con la normativa applicabile;
- permettere la tempestiva adozione della soluzione da attuare al fine di limitare o mitigare l'impatto della violazione dei dati personali sulle attività di business;
- usare i dati di "Risk events" in modo da migliorare l'identificazione e la valutazione del rischio;
- adempiere agli obblighi imposti dalla legge applicabile, dimostrando altresì all'Autorità l'impegno della Società nell'adozione di pratiche di gestione del rischio adeguate ai trattamenti effettuati.

3.1 Cos'è e cosa comporta un Data Breach

In relazione alla definizione fornita all'art. 4 comma 12 del GDPR, per Data Breach si intende qualsiasi **violazione di sicurezza** che comporti 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.

Secondo l'art. 32 comma 1 del GDPR, il titolare e i responsabili del trattamento mettono in atto adeguate misure tecniche ed organizzative che garantiscano un livello di sicurezza adeguato al rischio. Tra le altre, la Società deve:

- assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.

Partendo da tali definizioni, si identificano tre diverse categorie di violazione dei dati personali secondo i principi di sicurezza internazionalmente riconosciuti:

- *Violazione della confidenzialità:* si verifica nei casi in cui avvenga una divulgazione o un accesso non autorizzato o accidentale;

- *Violazione della disponibilità*: si verifica nei casi in cui avviene una perdita o distruzione dei dati in maniera accidentale e /o non autorizzata;
- *Violazione dell'integrità*: si verifica nel caso in cui l'evento riguardi la modifica non autorizzata o accidentale di dati personali.

La violazione di sicurezza è pertanto intesa come un atto accidentale, non autorizzato o intenzionale che comporti divulgazione, accesso, alterazione, distruzione o perdita di dati personali, andando quindi a corrompere uno o più principi di sicurezza delle informazioni.

Evento	**Descrizione dell'evento**	**Principio di sicurezza violato**
Distruzione / cancellazione dei dati personali	Indisponibilità irreversibile dei dati personali trattati dalla Società. La violazione può essere correlata a una cancellazione logica non autorizzata (ad esempio cancellazione dei dati, perdita irreversibile delle misure di sicurezza utilizzate per la protezione dei dati) e/o alla distruzione fisica (ad esempio rottura dei supporti), con l'impossibilità di ripristinare le informazioni.	Disponibilità
Perdita o furto di dati personali	Perdita di controllo sulle risorse di archiviazione fisica, come privazione, sottrazione, perdita di dispositivi o documenti cartacei. Una violazione può non sussistere quando è possibile escludere con ragionevole certezza l'accesso non autorizzato ai dati e se la perdita di memoria fisica non determina una perdita permanente di dati personali.	Disponibilità e riservatezza
Alterazione o modifica dei dati personali	Alterazione o modifica non autorizzata illegittima dei dati, che non è stata rilevata né modificata all'interno dei processi interni, causando così l'elaborazione o la divulgazione errata dei dati personali. Una alterazione illegittima può verificarsi in normali operazioni di elaborazione eseguite da personale autorizzato o in caso di modifiche fraudolente eseguite da soggetti non autorizzati.	Integrità
Divulgazione dei dati personali	Divulgazione non autorizzata o impropria di dati personali a terzi (persone fisiche o giuridiche, gruppi di soggetti, pubblico). Una violazione può non sussistere quando è possibile escludere con ragionevole certezza l'accesso non autorizzato ai dati.	Riservatezza
Accesso illegittimo o non autorizzato	Accesso alle informazioni personali elaborate dalla Società da soggetti non autorizzati.	Riservatezza

Una violazione di dati personali può rivelarsi un rischio che va a ledere i diritti dei soggetti impattati ed arrivare a provocare danni fisici, materiali o immateriali agli stessi. A titolo esemplificativo tra i danni si possono ricomprendere il furto di identità, perdite finanziarie, danno economico o sociale.

A tal fine, il titolare deve notificare la violazione dei dati personali all'Autorità, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza. Tale adempimento deve essere assolto solo nel caso in cui la violazione presenti un rischio per i diritti e le libertà degli Interessati ed il Titolare del Trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, tale rischio

sia improbabile (art. 33 par. 1 GDPR). Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

A titolo esemplificativo e non esaustivo si riportano alcuni esempi di eventi che potrebbero generare un Data Breach che può riguardare sia dati personali conservati in formato elettronico che cartaceo:

- furto di hardware contenente un archivio di dati personali;
- perdita di dati;
- interruzione delle linee dati (o linee telefoniche) che impedisce agli Interessati di contattare il titolare e avere accesso ai propri dati;
- attacco ransomware che provoca la crittografia di tutti i dati. Non sono disponibili back-up e i dati non possono essere ripristinati;
- comunicazione di dati personali di Interessati a destinatari errati (non incaricati del trattamento), ivi compresa la comunicazione a persone che non sono autorizzate ad avere accesso ai dati personali (e.g. parenti, amici o in ogni caso persone diverse dai Destinatari o soggetti a cui i dati personali devono essere comunicati per lo svolgimento dell'attività della Società);
- violazione dei siti web della Società a causa di cyber attacco, con conseguente estrazione di dati personali degli Interessati;
- qualsiasi installazione di software malevolo o virus scaricato sui dispositivi forniti dalla Società che può creare una perdita di disponibilità di dati personali, l'accesso abusivo a dati personali o la sottrazione di dati personali;
- violazione di caselle e-mail di dipendenti;
- furto di identità segnalato dalle forze dell'ordine;
- violazione di sicurezza fisica: furto o intrusione nei locali del titolare/responsabile;
- attacchi Denial of Service (DoS), che indicano un malfunzionamento dovuto ad un attacco informatico in cui si fanno esaurire deliberatamente le risorse di un sistema informatico che fornisce un servizio ai client, ad esempio un sito web su un web server, fino a renderlo non più in grado di erogare il servizio ai client richiedenti;
- attacchi Distributed Denial of Service (DDoS), che sta a significare il traffico in entrata che inonda la vittima proviene da molte fonti diverse;
- accesso non autorizzato ai dati;
- perdita o sottrazione di documenti cartacei o elettronici contenenti dati personali e.g. sottrazione o furto di un plico contenente dati di clienti o dipendenti;

3.2 Strutture coinvolte

Al fine di gestire in maniera ottimale e funzionale le eventuali violazioni di dati personali, è responsabile della gestione e valutazione delle eventuali violazioni dei dati personali il Comitato Privacy, che e assicura specifiche competenze rilevanti in merito alla protezione dei dati, alla sicurezza delle informazioni e dei sistemi informatici.

4 Le fasi di gestione di un Data Breach

4.1 Rilevazione

Il processo di analisi e gestione di una violazione dei dati personali ha inizio dalla segnalazione di un evento, di una anomalia o di un malfunzionamento che potrebbero potenzialmente configurare una violazione di dati personali. L'inizio della decorrenza del tempo utile alla comunicazione all'Autorità parte dal momento in cui si viene a conoscenza della violazione. È pertanto essenziale che in prima istanza il canale che attiva la segnalazione sia a conoscenza della presenza di dati personali nel set di informazioni impattate.
Fino alla conclusione formale della fase di rilevazione, non si può considerare quindi attestata la violazione.

La rilevazione della violazione è la fase in cui si devono identificare correttamente la tipologia di violazione dei dati personali, le categorie di soggetti coinvolti e la classificazione dell'incidente di sicurezza (riservatezza, indisponibilità, integrità).

Le violazioni possono pertanto rilevarsi sia internamente che esternamente alla Societàe pervenire alla stessa tramite segnalazione direttamente dal soggetto Interessato, da un dipendente, dalle Forze dell'Ordine o dall'Autorità, da un fornitore e in particolare dai responsabili esterni del trattamento, da altri canali quali ad esempio i media.

5.1.1 Procedura in caso di violazione dei dati rilevata da un soggetto interno alla Società

Ogni violazione rilevata internamente alla Società deve essere segnalata tempestivamente.

Non appena individuata la violazione, inoltre, il Destinatario coinvolto dovrà immediatamente - e comunque non oltre due ore dalla conoscenza o dal sospetto della violazione dei dati personali - darne comunicazione ad alla Società tramite posta elettronica inviando un'email all'indirizzo email dedicato databreach@falckrenewables.com fornendo le seguenti informazioni:

- la natura della violazione dei dati personali compresi e, ove possibile;
- le categorie e il numero approssimativo di individui i cui dati sono stati oggetto della Data Breach;
- le categorie e il numero approssimativo di registrazioni dei dati personali in questione; e
- ogni altra informazione volta ad individuare i dati oggetto del Data Breach e a mitigarne le conseguenze negative.

Entro le successive 24 ore dalla segnalazione, il Comitato Privacy dovrà organizzare una riunione supportato da ruoli specializzati in ambito tecnico / informatico in relazione al tipo di violazione avvenuta. La procedura dovrà proseguire quindi secondo le modalità di cui al successivo paragrafo 5.2.

5.1.2 Procedura in caso di violazione dei dati rilevata da un soggetto esterno alla Società

Ove un responsabile del trattamento - quali a titolo esemplificativo un fornitore di servizi , un agente, un partner commerciale o un consulente - rilevi o sospetti una violazione dei dati personali di cui la Società è Titolare del Trattamento, tale terzo non appena individuata la violazione dovrà immediatamente e senza ingiustificato ritardo ed in ogni caso entro 24 ore dalla conoscenza della violazione dei dati personali, darne comunicazione tramite posta elettronica all'indirizzo databreach@falckrenewables.com

Entro le successive 24 ore dalla segnalazione, il Comitato Privacy dovrà organizzare una riunione supportato da ruoli specializzati in ambito tecnico / informatico in relazione al tipo di violazione avvenuta, a cui potrà valutare di far partecipare anche un rappresentante del terzo al fine di avere maggiori dettagli in merito alla violazione e poter meglio definire le azioni da intraprendere per al fine di porre rimedio alla violazione de dati personali e per attenuare i possibili effetti negativi. La procedura dovrà proseguire quindi secondo le modalità di cui al successivo paragrafo 5.2.
I contratti con i terzi dovranno prevedere una nomina a responsabile del trattamento che prevedrà la procedura di cui al presente paragrafo 5 e gli obblighi di collaborazione previsti dal GDPR.

Per tutto il periodo di risoluzione dell'incidente le informazioni relative allo stesso e condivise tra i componenti del Comitato Privacy sono ritenute riservate e devono essere comunicate solo ed esclusivamente alle unità organizzative ed ai ruoli aziendali Interessati.

4.2 Gestione e verifica delle violazioni

A seguito del manifestarsi di un incidente, il Comitato Privacy dovrà avviare l'attività di gestione della violazione, identificando ed implementando la strategia di contenimento e contrasto più efficace finalizzata a minimizzare ogni ulteriore conseguenza tramite l'adozione di specifiche contromisure, e ad evitare un peggioramento della situazione, nonché provvedere a ripristinare tempestivamente la disponibilità e l'accesso ai dati personali.

Entro le successive 24 ore dalla segnalazione, il Comitato Privacy dovrà organizzare una riunione alla quale siano chiamate a partecipare anche tutte le Strutture operative ritenute necessarie ai fini della raccolta di informazioni circa la violazione dei dati personali (le "**Strutture**"). In tale riunione e nelle fasi propedeutiche alla stessa, le Strutture dovranno ottenere dai soggetti Interessati tutte le informazioni relative la violazione dei dati. Lo scopo della riunione sarà di:

- definire le cause, la natura e la portata del Data Breach, la quantità, la tipologia e il numero di Interessati a cui si riferiscono i dati personali oggetto della violazione, raccogliendo le informazioni da eventualmente notificare all'Autoritàai sensi dell'articolo 33 con il supporto del dipartimento IT e dei Responsabili Interni del trattamento;
- analizzare le azioni già intraprese e definire le azioni da intraprendere al fine di porre rimedio alla violazione de dati personali e per attenuare i possibili effetti negativi (ivi inclusa l'eventuale cancellazione remota dei dati contenuti nel dispositivo elettronico); e
- valutare il livello di rischio relativo alla violazione, come descritto nel successivo paragrafo 5.3, per determinare se una notifica all'Autorità ai sensi dell'articolo 33 del GDPR e una comunicazione agli Interessati ai sensi dell'articolo 34 del GDPR sono necessari.

Di seguito, si riporta un elenco (non esaustivo) delle attività previste per il contenimento dell'incidente:

- monitoraggio costante dell'evolversi della situazione; il monitoraggio del livello di criticità è un processo continuo e trasversale a tutte le fasi di gestione dell'incidente in quanto, in assenza di efficaci contromisure, l'evoluzione della situazione relativa ad un incidente in corso può peggiorare richiedendo il coinvolgimento progressivo di livelli aziendali superiori.
- Analisi del danno, lo stato degli asset impattati ed il volume dei dati violati.
- Monitoraggio del tempo impiegato e delle risorse necessarie.
- Contenimento dell'incidente, minimizzando gli impatti prodotti dallo stesso e prevenendo ulteriori danni tramite l'applicazione di contromisure di tipo tecnico procedurale organizzativo, le quali devono essere formalizzate e ne deve essere tenuta traccia.

- Implementazione delle necessarie attività idonee a ripristinare, ove possibile, la situazione precedente all'incidente.

Il Comitato Privacy verifica la segnalazione della potenziale violazione di dati personali, al fine di determinare la presenza effettiva di un rischio per i diritti e le libertà dei soggetti Interessati, verificando almeno:

- le informazioni relative alla natura dell'incidente (quando, dove, tipologia di violazione di sicurezza, sistemi e/o dispositivi oggetto di violazione);
- le categorie soggetti Interessati impattati;
- il volume di dati impattati;
- le misure adottate o da adottare per porre rimedio;
- i probabili rischi sui diritti e le libertà dei soggetti Interessati dalla violazione dei dati.
- le modalità e gli strumenti di risoluzione dell'incidente.

Si ritiene che la Società possa acquisire un grado di ragionevole certezza dell'avvenuta violazione dei dati personali in presenza di:

- informazioni concrete relative alla violazione dei dati personali;
- evidenze della perdita di confidenzialità, integrità, disponibilità dei dati personali;
- conseguenze sicuramente derivanti dall'incidente di sicurezza sui diritti e le libertà dei soggetti Interessati.

4.3 Livello di rischio

Nella definizione del livello di rischio devono essere tenute in considerazione tutte le potenziali conseguenze e i probabili effetti negativi che, ragionevolmente, potrebbero impattare i soggetti Interessati.

Sulla base delle indicazioni del Gruppo di Lavoro ex Articolo 29 "*Guidelines on personal data breach notification under Regulation 2016/679*", pubblicate il 6 Febbraio 2018, ed in particolare del documento predisposto da ENISA "Recommendations for a methodology of the assessment of severity of personal Data Breaches", Working Document, v1.0, December 2013, gli elementi da considerare nella valutazione sono:

- ***Contesto del Trattamento (CT):*** il criterio tiene in considerazione la tipologia di dati personali coinvolti nella violazione dei dati in correlazione a fattori specifici del trattamento che potrebbero aggravare o attenuare l'impatto sul soggetto Interessato (volume dei dati violati, circostanze specifiche della Società, circostanze specifiche del soggetto Interessato, disponibilità pubblica del dato, accuratezza del dato). Il valore del criterio è compreso tra 1 e 4.
- ***Facilità di Identificazione (FI):*** il criterio considera la possibilità di identificare puntualmente un soggetto sulla base del dato oggetto di violazione, considerando anche i casi di violazione contemporanea di più di una tipologia di dati dello stesso soggetto. Il criterio è utilizzato come valore correttivo del contesto del trattamento, in quanto minore è il livello di identificabilità dell'individuo sulla base degli identificatori comuni, minore risulterà la gravita della violazione.
- ***Circostanze della violazione (CV):*** specifiche circostanze della violazione in correlazione alla categoria della violazione (perdita di integrità, riservatezza, disponibilità).

Tenendo conto di questi elementi, è possibile classificare tutti gli eventi. Per ciascuno dei criteri sopra riportati è stato definito un insieme di valori da selezionare in relazione alle caratteristiche della violazione oggetto di analisi.

Il risultato finale viene convertito in una scala qualitativa a 4 valori (Basso, Medio, Alto, Molto Alto). A seconda del livello di rischio ottenuto si identificano:

- la presenza o meno di pregiudizi per gli Interessati oggetto di violazione;
- l'esigenza di effettuare comunicazioni verso l'Autorità e/o gli Interessati.

Gravità della violazione dei dati (severity) - tabella di riepilogo	
BASSA	Gli Interessati non saranno Interessati o potrebbero incontrare alcuni lievi inconvenienti, superabili senza particolari problemi (tempo trascorso a reinserire informazioni, fastidi, irritazioni, ecc.).
MEDIA	Gli Interessati possono incontrare notevoli disagi, che saranno in grado di superare pur con alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici minori, ecc.).
ALTA	Gli Interessati possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, lista nera da parte delle banche, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).
MOLTO ALTA	Gli individui possono incontrare conseguenze significative, o addirittura irreversibili, che non possono superare (difficoltà finanziarie come debito sostanziale o incapacità lavorativa, disturbi psicologici o fisici a lungo termine, morte, ecc.).

Le metriche e la metodologia utilizzata consentono di classificare come bassi tutti gli eventi che, pur potendo formalmente presentare caratteristiche di violazione ai dati personali, non configurano in alcun modo pregiudizio per gli Interessati e per i quali non si reputa necessaria alcuna comunicazione, né verso l'Autoritànè verso gli Interessati stessi.
In generale, analizzando la classificazione delle violazioni si considera che:

- in caso di possibile ***violazione della riservatezza o dell'integrità***, se i dati personali oggetto di violazione non sono intellegibili, sono stati anonimizzati o pseudonimizzati, l'impatto associato alla violazione potrebbe essere basso e potrebbe non essere necessaria per essere notificata all'Autoritànè all'Interessato;
- in caso di possibile ***perdita di disponibilità***, se sono presenti copie o backup dei dati, l'impatto associato alla violazione potrebbe essere basso e potrebbe non essere necessaria per essere notificata all'Autoritànè all'Interessato.

Se la Società̀non riuscisse a valutare entro 48 ore dalla rilevazione la violazione occorsa per mancanza di informazioni precise, verrà eseguita un'analisi di impatto che prenda in considerazione il *worst case* in modo da riuscire ad eseguire la comunicazione verso l'Autorità entro le 72 ore dalla conoscenza della violazione.

Qualora il Data Breach verificatosi abbia una gravità alta o molto alta, tale da richiedere la notifica all'Autoritàe ai sensi del successivo paragrafo 5.4, lo stesso sarà qualificato come evento di crisi ai fini della Procedura di *Crisis Communication management* e sarà coinvolto il Crisis Team secondo quanto prescritto in tale procedura.

4.4 Notifica

Come precedentemente detto, appena il titolare è ragionevolmente certo che la violazione potrebbe comportare un rischio per i soggetti Interessati, ha il dovere di notificare all'Autorità tutte quelle violazioni di dati personali che possono determinare un rischio per i diritti e le libertà degli Interessati.

Nello specifico tale notifica deve contenere almeno:

- una descrizione della 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;
- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere maggiori informazioni;
- una descrizione delle probabili conseguenze della violazione dei dati personali;
- una descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Nel caso in cui le informazioni non siano reperibili entro le 72 ore, è possibile fornirle in fasi successive senza ulteriore ingiustificato ritardo e scegliere una delle due opzioni di seguito riportate:

- *Notificazione in fasi*: a causa della complessità della violazione o per il prolungarsi delle analisi di investigazione della violazione di sicurezza, il titolare può fornire, entro le 72 ore una prima descrizione del contesto della violazione al fine di allertare l'Autorità. Le informazioni mancanti saranno comunicate in fasi successive tramite ulteriori notificazioni idonee a delineare il panorama completo ed esaustivo della violazione dei dati personali.
- *Notifica con dati approssimati*: approssimazione di determinate informazioni che potranno essere dettagliate nelle fasi successive (es. approssimazione numero delle persone fisiche coinvolte nella violazione dei dati personali).

Generalmente, qualora una notifica non venga inviata entro le 72 ore, la notifica deve comprendere le motivazioni del ritardo sulla base delle specifiche circostanze.
L'obbligo di notifica verso l'Autorità e/o gli Interessati non risulta applicabile nel momento in cui la Società dimostra, in accordo con il principio di responsabilizzazione, che la violazione non comporta rischi per i diritti e le libertà degli Interessati.

L'identificazione dell'inesistenza dei rischi per i diritti e le libertà dei soggetti Interessati deve prendere in considerazione:

- il risultato della valutazione del Data Breach;
- tutte le possibili conseguenze attuali o future derivanti dalla perdita dei principi di sicurezza, nonché della protezione dei dati: integrità, disponibilità, riservatezza;
- le misure tecniche ed organizzative implementate precedentemente e conseguentemente alla violazione dei dati personali al fine di tutelare il soggetto Interessato riducendo l'impatto della violazione sulle persone fisiche, e per ripristinare tempestivamente la disponibilità e l'accesso ai dati personali.

5.4.1 Notifica al soggetto Interessato

Qualora il livello del rischio derivante dalla violazione dei dati personali a seguito della valutazione di cui al paragrafo 5.3, risulti elevato o molto elevato per i diritti e le libertà della persona fisica cui i dati personali sono stati colpiti dall'evento, il titolare (ove non sussistano i presupposti per non procedere con la comunicazione) ha l'obbligo di comunicare la notizia dell'evento anche alle persone fisiche di cui i dati risultino coinvolti nella violazione. La notifica ha lo scopo di rendere il soggetto Interessato in grado di prendere le precauzioni necessarie per attenuare potenziali effetti negativi e deve essere obbligatoriamente inviata senza indebito ritardo.
Nella definizione e predisposizione di una comunicazione adeguata nei confronti dei soggetti Interessati colpiti dalla violazione, devono essere prese in considerazione:

- le informazioni necessarie ed idonee al contesto che devono essere fornite al soggetto Interessato;
- le modalità di effettuazione.

La comunicazione ai soggetti Interessati deve almeno contenere:

- la descrizione della natura della violazione dei dati personali;
- la descrizione delle probabili conseguenze delle violazioni dei dati personali;
- la descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi;
- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere maggiori informazioni;
- ove possibile o in caso di specifico suggerimento da parte dell'Autorità di controllo, l'elenco di buone prassi e/o specifiche misure da adottare da parte delle persone fisiche colpite dalla violazione, al fine di attenuare le conseguenze negative,
- ogni altra informazione ritenuta utile.

I contenuti elencati dovranno essere veicolati al soggetto Interessato tramite canali diretti (esempio: per mezzo di e-mail, sms), adottando una comunicazione chiara, trasparente ed esplicita. La scelta della modalità di comunicazione dovrà tenere in considerazione l'accessibilità dei soggetti Interessati a formati diversi, e, ove necessario, le diversità linguistiche dei destinatari.
Sulla base delle specifiche circostanze del caso, dovrà essere scelta la modalità di comunicazione capace di massimizzare la ricezione delle informazioni da parte del soggetto Interessato in maniera corretta, semplice ed agevole, garantendo al contempo la sicurezza del trasferimento delle informazioni.
La comunicazione deve essere effettuata non appena ragionevolmente possibile, tenendo in considerazione gli orientamenti in materia derivanti dall'Autorità, le conseguenze che potrebbero derivare dallo specifico contesto della violazione nonché dalla natura dei dati e dalle finalità del trattamento, le conseguenze che potrebbe impattare la gestione dell'incidente e il contenimento della violazione.

La Società non è tenuta a comunicare la violazione ai soggetti Interessati, qualora venga soddisfatta una delle seguenti condizioni:

- sono state implementate le misure tecniche e organizzative adeguate di protezione e tali misure sono tate applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi (esempio: cifratura);
- il titolare, successivamente alla rilevazione dell'evento, ha adottato, tempestivamente, misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli Interessati;
- qualora la modalità di comunicazione diretta risulti un sforzo sproporzionato per il Titolare del Trattamento di cui i dati sono stati colpiti dalla violazione, il titolare può adottare canali di comunicazione pubblica, purché risulti una modalità comunicativa efficace da un punto di vista della correttezza, trasparenza, e purché non leda ulteriormente la privacy del soggetto Interessato.

4.5 Registro dei Data Breach

In conformità al Regolamento, 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, in un registro delle violazioni. Tale documentazione consente all'Autorità di verificare la conformità delle valutazioni, delle precauzioni e decisioni prese in relazione all'articolo 33 del GDPR.

Tale documento è mantenuto ed implementato dal Privacy Expert o in sua vece dal CDT&IO che ne garantiscono la completezza, l'aggiornamento e l'integrità delle informazioni ivi contenute.
Si sottolinea che, nel caso in cui l'evento segnalato non è stato valutato come violazione dei dati personali, dovranno essere annotate le motivazioni che hanno portato a tale tipologia di valutazione.

Allegato E
Data Retention Policy

1. Introduzione e finalità

La presente Policy sulla Conservazione dei Dati (la "**Policy**") è volta ad illustrare gli obblighi a cui tutti i dipendenti e collaboratori (di seguito congiuntamente definiti gli "**Destinatari**") devono attenersi con rifermento ai tempi di conservazione dei dati personali al fine di garantire la conformità delle società del Gruppo al Regolamento (UE) 2016/679 del Parlamento e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché la libera circolazione di tali dati (di seguito il "**Regolamento Privacy**" o "**GDPR**").

2. A chi si applica la presente Policy?

La Policy si applica a:

a) tutti i documenti, archivi o registri creati (di seguito i "**Document**i") o ricevuti dal Gruppo, indipendentemente dal mezzo o formato (e.g. elettronico, e-mail, immagine, cartaceo, ecc.), che contengono dati personali;

b) in tutti gli ambienti fisici dove i Documenti sono conservati (ivi incluse le strutture gestite da eventuali fornitori di servizi);

c) tutti i dipendenti e collaboratori di qualsivoglia unità organizzativa del Gruppo e dei fornitori.

Ove la presente Policy non faccia riferimento ad uno specifico documento, archivio o registro, sarà necessario conformarsi ai seguenti principi:

a) i dati personali dovranno essere conservati per il tempo strettamente necessario a soddisfare le finalità per le quali i dati sono stati raccolti;

b) ove i dati personali contenuti nel Documento siano cancellati o diversamente anonimizzati, tale Documento potrà essere conservato per un periodo di tempo più lungo (fatte salve le limitazioni imposte da diversa disposizione di legge o eventuali accorgimenti dovuti alla sensibilità del documento);

c) è generalmente vietato conservare i Documenti per un periodo indefinito di tempo, ad eccezione di specifiche circostanze.

d) Dove posso ottenere maggiore informazioni con riferimento alla presente Policy?

Per qualsivoglia chiarimento sulla presente Policy potrai fare riferimento al Privacy Expert del Gruppo che potrà essere contattato al seguente indirizzo privacyexpert@falckrenewables.com

e) Distruzione dei Dati

I Documenti che superano i termini di conservazione di cui alla seguente tabella potranno essere distrutti a seguito della approvazione del Privacy Expert. In ogni caso, la distruzione prematura del Documento è espressamente proibita.

TABELLA DI CONSERVAZIONE DEI DATI

Descrizione della previsione normative con riferimento alla conservazione di dati personali	**Natura dei documenti contenenti dati personali**	**Periodo di conservazione**	**Commenti**
PRINCIPIO GENERALE - Limitazione alla conservazione dei dati personali	Qualsivoglia documento contenente dati personali	I Documenti devono essere conservati in una forma che permetta la identificazione degli interessati per un tempo non superiore all'adempimento delle finalità per cui i dati sono stati raccolti o comunque trattati. Tuttavia, ove le norme applicabili al caso concreto prevedano un termine maggiore, quest'ultimo dovrà considerarsi prevalente.	Tale principio è applicabile a qualsivoglia trattamento di dati personali. Con riferimento a contratti contenenti dati personali, è consigliabile conservare i Documenti fino ad un periodo di 10 anni dal termine del contratto stesso probatorie in caso di controversia.
HEALTH AND SAFETY			
Registro di controllo delle attrezzature di lavoro.	Il Registro di controllo delle attrezzature di lavoro è un documento contenente la descrizione dello stato di conservazione degli strumenti lavorativi.	A tempo indeterminato. Il documento deve essere sempre disponibile in caso di ispezioni delle autorità.	

Registro di esposizione e cartelle sanitarie e Registro degli esposti e degli eventi accidentali relativi ai dipendenti che possono svolgere attività pericolose o in ambienti insalubri (i.e. attività che presuppongono l'utilizzo di sostanza pericolose).		Da conservare fino al termine del rapporto contrattuale. E' tuttavia consigliabile (i) tenere aggiornati tali registi con cadenza periodica (idealmente con cadenza annuale) e (ii) conservare i registri, almeno per 10 anni dalla cessazione del rapporto di lavoro.	Tale registro dovrà essere disponibile in caso di ispezioni delle autorità

Dovere di redigere una valutazione del rischio relativo alle attrezzature di lavoro e delle sostanze o miscele chimiche impiegate. La valutazione del rischio è volta ad identificare: (i) qualsivoglia rischio per la sicurezza e la salute durante l'attività lavorativa, (ii) misure di prevenzione e di protezione attuate e dei dispositivi di protezione individuali adottati; (iii) il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza; (iv) l'individuazione delle procedure per l'attuazione delle misure da realizzare; (v) l'indicazione del nominativo del responsabile del servizio di prevenzione e protezione, del rappresentante dei lavoratori per la sicurezza o di quello territoriale e del medico competente che ha	Documentazione circa la valutazione dei rischi.	A tempo indeterminato.	

partecipato alla valutazione del rischio, (vi) l'individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale.			
Dovere di conservare tutti i dati relativi alle visite mediche del dipendente, ove necessario.	Registro delle visite mediche.	Non vi è alcuna indicazione con riferimento ai tempi di conservazione di tale documento. Tuttavia, è consigliabile (i) aggiornare il registro con cadenza periodica (almeno annuale) e (ii) conservare il registro per 10 anni dalla cessazione del rapporto di lavoro.	
ACCOUNTING e AUDITING / DIRITTO SOCIETARIO			
Dovere di conservare libri, scritture contabili e corrispondenza d'affari.	Libri, scritture contabili e corrispondenza d'affari (e.g. il libro giornale, i libri ausiliari, i giustificativi che documentano gli elementi importanti delle iscrizioni e tutti gli scritti inviati, ricevuti o interni che abbiano natura e rilevanza contabile).	10 anni dalla data in cui tali documenti sono redatti - tale termine può essere più ampio (i) per motivi fiscali e (ii) in caso di giudizio ove sia stata presentata una richiesta di produzione di tali documenti.	Devono essere osservate le indicazioni circa la modalità di redazione dei libri e delle scritture contabili previste dal Codice Civile.
DIRITTI DI PROPRIETA' INTELLETTUALE			

Documentazione relativa a marchi, brevetti, nomi a dominio, segreti industriali ecc.		Non sussiste un termine per la conservazione dei documenti relativi ai diritti di proprietà intellettuale. Tuttavia, per finalità probatorie suggeriamo di conservare tali documenti a tempo indeterminato (e.g. certificati di registrazione dei marchi, brevetti, ecc.)	
ANTIRICICLAGGIO			
Dovere di conservare i documenti, i dati e le informazioni utili a prevenire, individuare o accertare eventuali attività di riciclaggio o di finanziamento del terrorismo e a consentire lo svolgimento delle analisi effettuate, nell'ambito delle rispettive attribuzioni, dalla Unità di Informazione Finanziaria o da altra Autorità competente.	Documenti e dati raccolti durante la verifica dei clienti e/o fornitori.	10 anni dalla fine del rapporto continuativo.	
DOCUMENTI HR			
Dovere di conservare (I) i dati dei dipendenti (i.e. il nome e cognome, il codice fiscale), (ii) il numero totale	Libro unico.	5 anni dalla data dell'ultima registrazione.	Durante il periodo di conservazione i dati devono essere conservati in

dei dipendenti e la qualifica ed il livello professionale, (iii) le relative posizioni assicurative.			conformità con le norme applicabili in materia di protezione dei dati personali. Con riferimento ai dati/documenti relativi agli ex dipendenti, questi devono essere inclusi in un file elettronico accessibile esclusivamente al dirigente del dipartimento delle risorse umane o altro soggetto dallo stesso espressamente incaricato e al Consiglio di Amministrazione ed eventuali altri organi di governo aziendale autorizzati.
Dovere di conservare tutti i dati relativi alle procedure di assunzione e del rapporto di lavoro.	Documentazione su procedure di assunzione, sul contratto di lavoro e relativa documentazione.	Non sussiste alcuna specifica previsione in proposito. Tuttavia è consigliabile conservare tali documenti per un periodo di almeno 10 anni dalla cessazione del rapporto di lavoro. I dati dei candidati saranno conservati, nel caso di candidature inviate per posizioni determinate, fino a 12 mesi dalla chiusura della selezione, nel caso di candidature spontanee, fino a 24 mesi dalla data di raccolta dei dati.	
Dovere di conservare tutti i dati relativi alle contribuzioni corrisposte per i dipendenti.	Buste paga e altri documenti relativi a pagamenti.	Le buste paga e analoghi documenti relativi alla retribuzione del dipendente devono, quindi, esser conservati per un periodo di 5 anni dall'ultima registrazione. Tuttavia è consigliabile conservare tali informazioni per un periodo di almeno 10 anni dalla cessazione del rapporto di lavoro.	
Ad eccezione del caso in cui sussistano altre	Altri dati dei dipendenti.	Al fine di proteggere gli interessi della società in caso di azioni da parte dei dipendenti a seguito della cessazione del rapporto di	

specifiche previsioni che prevedano diversamente, i dati personali dei dipendenti (ivi inclusi i dati contenuti nei contratti di lavoro e i contratti di lavoro stessi) devono essere conservati per un periodo non superiore a quanto necessario per le finalità per i quali i dati sono stati raccolti.		lavoro, è consigliabile conservare i dati almeno per un periodo di 10 anni a seguire della data di cessazione del rapporto di lavoro.	
Dovere di conservare tutti i dati relativi alle posizioni di previdenza e alle deduzioni fiscali.	Dati relativi alle posizioni di previdenza e alle deduzioni fiscali	Tali informazioni sono soggette all'obbligo di conservazione quinquennale. Tuttavia è consigliabile conservarle per un periodo di almeno 10 anni dalla cessazione del rapporto di lavoro.	
Dovere di conservare tutti i dati relativi a (i) certificati famigliari e documenti relativi all'Assegno Nucleo Familiare e (ii) qualsivoglia pagamento effettuato all'I.N.A.I.L.- Istituto Nazionale per l'assicurazione contro gli infortuni sul lavoro.	Certificati famigliari e documenti relativi all'Assegno Nucleo Familiare e (ii) qualsivoglia pagamento effettuato all'I.N.A.I.L.	Tali informazioni sono soggette all'obbligo di conservazione quinquennale. Tuttavia è consigliabile conservarle per un periodo di almeno 10 anni dalla cessazione del rapporto di lavoro.	
Limite alla conservazione delle immagini di videosorveglianza	Video relativi agli individui.	Ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria.	
Limite alla conservazione delle comunicazioni di posta elettronica degli ex-dipendenti	Comunicazioni contenute nella casella di posta elettronica degli ex-dipendenti.	Per la posta elettronica in entrata/uscita dell'ex dipendente: 3 mesi dalla cessazione del rapporto lavorativo per assicurare la continuità dell'attività lavorativa e del *business aziendale*. Per le sole comunicazioni archiviate dall'ex-dipendente all'interno del sistema di gestione documentale in quanto rilevanti per la continuità	

		aziendale: 10 anni dalla cessazione del rapporto lavorativo. In caso di comprovate e concrete esigenze di tutela o esercizio di un diritto della Società in sede giudiziale o stragiudiziale o richieste delle autorità: fino alla conclusione dell'ultimo grado di giudizio e/o conclusione della fase stragiudiziale e comunque mai oltre 10 anni dalla cessazione del rapporto lavorativo.	
Limite alla conservazione dei dati personali dei dipendenti raccolti tramite i badge di accesso	Dati accesso mediante badge Dati accesso mediante badge.	5 anni dalla raccolta 5 anni dalla raccolta.	
Dovere di conservare tutti i dati relativi alla presenza al lavoro dei dipendenti.	Calendario presenze.	5 anni dall'ultima registrazione.	
DOCUMENTI RELATIVI ALLE ATTIVITA' DI MARKETING			
Dati raccolti e trattati per finalità di marketing.	Qualsiasi documento rilevante.	Non sussiste alcuna specifica previsione in proposito. Tuttavia, secondo l'orientamento è possibile conservare tali dati, previo consenso da parte degli interessati, per i 24 mesi successivi alla raccolta dei dati	
Dati trattati per finalità di profilazione.	Qualsiasi documento rilevante.	Non sussiste alcuna specifica previsione in proposito. Tuttavia, secondo l'orientamento, è possibile conservare tali dati, previo consenso degli interessati, per i 24 mesi successivi alla raccolta dei dati.	
LOG DI SISTEMA			
Registrazione di log di Sistema	File elettronici	Il periodo di conservazione dei dati è di 6 mesi dal momento della raccolta.	