



REGIONE AUTONOMA
DELLA SARDEGNA

M.O.P. - MODELLO ORGANIZZATIVO PRIVACY

Applicazione del Regolamento Europeo 679/2016
("GDPR") in materia di protezione dei dati personali

Nome documento:	MOP – Modello Organizzativo Privacy	Versione - Revisione	01.01
Redatto da:	Data Protection Officer	Firma RPD/DPO (referente)	<i>Pesuyali Nicolo</i>

SOMMARIO

FINALITÀ DEL DOCUMENTO	4
TERMINI E DEFINIZIONI	5
STRUTTURA ORGANIZZATIVA PRIVACY: RUOLI E RESPONSABILITÀ	8
Titolare del Trattamento	9
Designato del Titolare (Responsabile Delegato alla tutela dei dati personali)	9
Referenti Data Protection (se nominati).....	11
Autorizzato al trattamento.....	12
Amministratore di Sistema (AdS, se nominato).....	13
Responsabile della Protezione dei Dati (RPD) - DPO Data Protection Officer	14
Responsabile del Trattamento.....	16
Consulente Privacy / Privacy Officer (se presente).....	18
PRINCIPI GENERALI PER IL TRATTAMENTO DEI DATI.....	20
Trattamento di dati personali e condizioni di liceità	20
Privacy by design e Privacy by default.....	21
Principio di minimizzazione	22
Periodo di conservazione dei dati personali	22
Accesso ai dati personali.....	22
Misure di sicurezza	22
Trasferimento di dati personali all'estero	23
I DIRITTI DELL'INTERESSATO	24
IL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO	26
IL RESPONSABILE DEL TRATTAMENTO	27
INFORMATIVA IN MATERIA DI PROTEZIONE DATI E RICHIESTA DI CONSENSO	29
L'Informativa in materia di protezione dati.....	29
L'Informativa diretta.....	29
L'Informativa indiretta	30
La richiesta di consenso.....	30

*Il consenso per l'accesso ai servizi on-line.....	31
VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA).....	32
VIOLAZIONE DEI DATI PERSONALI (DATA BREACH).....	33
FORMAZIONE.....	34
LE SANZIONI.....	35
Violazioni da parte del personale della Società.....	35
Violazioni da parte del Responsabile del trattamento.....	35
ALLEGATI.....	36
POLITICHE GENERALI PER L'UTILIZZO DI DISPOSITIVI E STRUMENTI INFORMATICI..	36
Titolarità, autorizzazione e finalità di utilizzo degli strumenti informatici.....	36
Postazioni di lavoro.....	36
SISTEMI DI PROTEZIONE DEI DATI.....	40
Credenziali di autenticazione.....	40
Scelta della password.....	40
Antivirus.....	42
Sistemi di backup.....	42
OPERATIVITÀ SU BANCHE DATI.....	43
SERVIZI DI RETE.....	43
UTILIZZO DI INTERNET.....	45
POSTA ELETTRONICA.....	47
COLLEGAMENTO REMOTO.....	49
*SISTEMI DI TELEFONIA.....	49
ACCESSO AI SISTEMI.....	49
PROTEZIONE DEI DATI - TECNICHE DI SOTTRAZIONE.....	50
Il social engineering.....	50
L'E-mail phishing.....	50
POLITICHE GENERALI PER L'UTILIZZO DEGLI ARCHIVI CARTACEI.....	52

FINALITÀ DEL DOCUMENTO

Il presente documento descrive il “Modello Organizzativo” di cui si è dotata la società CARBOSULCIS SPA (di seguito “Società” o “Titolare”) in riferimento ai trattamenti di dati personali di soggetti persone fisiche, in coerenza alla normativa vigente, tra cui, in particolare, il Regolamento Europeo 679/2016 (di seguito, per brevità, “Regolamento” o “GDPR”), del Decreto Legislativo 196/2003 (di seguito anche “Codice Privacy”) come novellato dal Decreto Legislativo 101/2018.

All'interno del presente documento sono descritte le strutture organizzative della società, i ruoli e le responsabilità dei soggetti che effettuano i trattamenti, nonché i principi che regolamentano e disciplinano le modalità di esecuzione delle attività di trattamento di dati personali eseguite dalla Società per le finalità di trattamento di cui essa è Titolare (o Contitolare o Responsabile).

Il Modello Organizzativo ivi descritto ha l'obiettivo di formalizzare le linee guida che la Società ha adottato e intende applicare per assicurare che i trattamenti di dati personali siano effettuati in conformità alle disposizioni previste dalla normativa in materia, in particolare:

- a) siano acquisiti e trattati su idonea base giuridica, per scopi determinati, espliciti e legittimi;
- b) siano trattati solo per le finalità proprie della Società e in maniera non eccedente alle stesse;
- c) siano trattati nel rispetto dei diritti e della dignità degli Interessati;
- d) siano protetti dal rischio, anche solo potenziale, di distruzione, perdita, modificazione, rivelazione non autorizzata, accesso non autorizzato, non esattezza e non adeguatezza rispetto alle finalità per cui sono trattati;
- e) siano comunicati legittimamente all'interno e/o all'esterno della Società.

Le politiche presenti nel presente Modello si applicano a tutti i dipendenti e collaboratori di qualsiasi genere (Stagisti, Tirocinanti, Volontari, etc) della Società. A tal fine, esse si assicurano che, al momento dell'assunzione/instaurazione del rapporto, ciascun dipendente e / o collaboratore riceva una copia del presente documento e/o ne prenda visione.

Per la descrizione e la trattazione di dettaglio dei processi connessi ai trattamenti di dati personali, quali, a titolo esemplificativo e non esaustivo, la gestione delle richieste di esercizio diritti dell'interessato o la gestione e notifica delle violazioni di dati personali (Data Breach), si fa rimando ai Disciplinari/Policy adottati dalla Società.

Per eventuali dubbi in merito al trattamento dei dati personali, i soggetti Autorizzati ai trattamenti (così come descritti nei successivi capitoli) potranno rivolgersi al Responsabile Protezione Dati / Data Protection Officer (RPD/DPO) della Società.

Il presente documento viene aggiornato su proposta del Titolare, del Designato del Titolare e/o del Responsabile della Protezione dei Dati in conseguenza di modifiche normative o per esigenze organizzative/operative.

TERMINI E DEFINIZIONI

Al fine di una piena comprensione e attuazione del presente documento, si riportano i principali termini utilizzati e le relative definizioni:

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'articolo 51 GDPR.

Consenso dell'interessato: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

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.

Dato personale: qualunque 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, generica, psichica, economica, culturale o sociale.

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.

Destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.

Disponibilità: proprietà del dato di essere presente e utilizzabile nei tempi, nei luoghi e nelle modalità adeguati alle necessità operative.

Evento di sicurezza: qualsiasi occorrenza anomala in ambito Sicurezza Informatica che non sia un falso positivo ed osservabile sia attraverso piattaforme di monitoraggio sia attraverso interazioni umane e che, a valle di una fase di triage, può essere identificata come incidente di sicurezza.

Falso positivo: evento che si rivela, dopo attenta analisi, non impattante in termini di sicurezza.

Impatto: effetto causato dall'avvenuta violazione della sicurezza sugli asset ICT e/o sul patrimonio informativo della Società.

GDPR: Regolamento Europeo 679/2015 in materia di protezione dati personali.

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

Interessato: persona fisica cui si riferiscono i dati trattati dal Titolare o dal Responsabile.

Designato/Delegato al trattamento: la persona fisica che, secondo l'organizzazione aziendale, ricopre un ruolo gestionale e di responsabilità all'interno dell'azienda che determina specifiche modalità organizzative rispetto ad uno o più trattamenti.

Autorizzato al trattamento: la persona fisica, espressamente autorizzata/incaricata, che opera sotto l'autorità del Titolare, con specifici compiti e funzioni connessi al trattamento dei dati personali.

Referente privacy: la persona fisica (o gruppo) che operativamente si interfaccia con il DPO e funge da collegamento tra lo stesso e il Titolare (nonché con i soggetti che a vario titolo operano all'interno della struttura del Titolare).

Limitazione del trattamento: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro.

Minaccia: tipo di azione, sia deliberata che accidentale, che può in qualsiasi modo arrecare direttamente o indirettamente un danno all'integrità, alla riservatezza o disponibilità di un dato.

Organizzazione internazionale: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

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 indentificata o identificabile.

Rappresentante: la persona fisica o giuridica stabilita nell'Unione che, designata dal Titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27 GDPR, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento.

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.

RPD/DPO (Responsabile Protezione Dati/Data Protection Officer): figura professionale con particolari competenze, il cui compito principale è l'osservazione, la valutazione e l'indirizzo sulle modalità di trattamento dei dati allo scopo di far rispettare le normative europee e nazionali.

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.

Rilevazione: qualsiasi segnalazione di potenziale evento di sicurezza o occorrenza osservabile in un sistema o rete.

Riservatezza: proprietà del dato di essere conoscibile solo ad alcuni soggetti, normalmente individuati dal "proprietario" del dato stesso, e non ad altri.

Stabilimento principale:

a) Per quanto riguarda un Titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del Titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale.

b) Con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento.

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.

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.

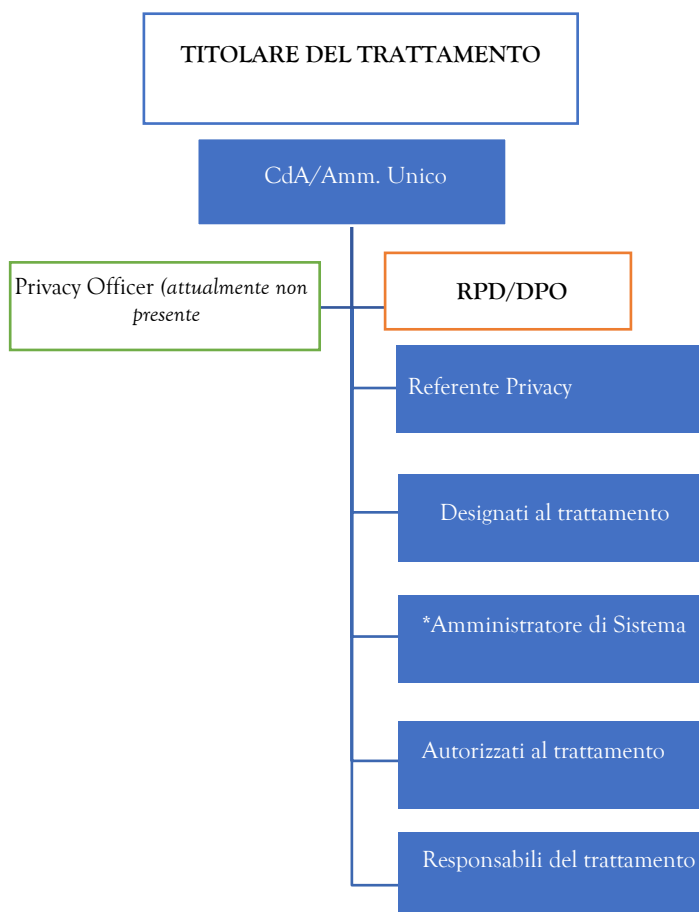
WP29: organismo consultivo e indipendente, composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro dell'Unione Europea, dal GEPD (Garante europeo della protezione dei dati), nonché da un rappresentante della Commissione Europea - ora sostituito dall'European Data Protection Board (EDPB).

STRUTTURA ORGANIZZATIVA PRIVACY: RUOLI E RESPONSABILITÀ

CARBOSULCIS SPA ha definito un assetto organizzativo volto alla protezione dei dati personali (Data Protection), progettato in ottemperanza al principio di Responsabilizzazione (“Accountability”) al fine di conformarsi in modo appropriato alle prescrizioni del GDPR.

La Società, in qualità di Titolare del Trattamento, può prevedere, nell’ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche espressamente designate che operano sulla base di un rapporto di lavoro dipendente o di collaborazione. In base a tale principio, la stessa individua le modalità per Autorizzare al trattamento dei dati personali le persone che operano sulla base di un rapporto di lavoro dipendente o di collaborazione.

Di seguito è riportata una sintesi grafica dell’Assetto Organizzativo “Data Protection”, con evidenza dei singoli ruoli e delle relative interdipendenze gerarchiche.



Titolare del Trattamento

Il Titolare del Trattamento dei dati personali è, ai sensi dell'art. 4 e 24 del GDPR, “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” (“Titolare”).

Alla luce della suddetta definizione, la società CARBOSULCIS SPA, con sede legale in Località Monte Sinni (Nuraxi Figus) - 09010 Gonnosa (Carbona-Iglesias/CI) - Sardegna/Italy, C.F./P.IVA: 00456650928, Tel: 0781.4921___ - E-mail: segreteriagenerale@carbosulcis.eu - PEC: appalti@pec.carbosulcis.eu, è TITOLARE per i trattamenti di dati personali mappati nel “Registro delle attività di trattamento” e relativamente ai quali determina finalità e modalità di trattamento.

Il Titolare è la struttura nel suo complesso e cioè il soggetto al quale competono le scelte di fondo sulla raccolta e sull'utilizzazione dei dati personali. Il Titolare agisce per mezzo degli Organi statutari nel loro complesso o del soggetto (Presidente CdA / Amministratore Unico) a cui i relativi poteri in materia di protezione di dati personali sono stati pro tempore attribuiti dagli Organi Direttivi.

L'art. 24, GDPR, stabilisce la responsabilità generale del Titolare per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. In particolare, il Titolare deve essere in grado di dimostrare la conformità delle attività di trattamento con il GDPR stesso (Accountability) e deve mettere in atto misure adeguate ed efficaci volte a garantire ciò. Tali misure devono tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.

Inoltre, al fine di dimostrare la conformità delle sue azioni con il GDPR, il Titolare deve adottare politiche interne ed attuare misure che soddisfino i principi della “Protezione dei dati di Default” e “fin dalla progettazione”.

Il Titolare delega lo svolgimento di parte delle proprie attività a soggetti interni in veste di Delegato/Designato del Titolare e di Autorizzati, nonché nomina Responsabili del Trattamento i soggetti esterni che, nell'esecuzione di un servizio a favore della Società, trattano i dati personali in titolarità / responsabilità di quest'ultima. Il Titolare ha la responsabilità di individuare al riguardo soggetti che presentino garanzie sufficienti per mettere in atto le prescritte misure tecniche e organizzative adeguate.

Designato del Titolare (Responsabile Delegato alla tutela dei dati personali)

Il Designato (ex art. 2-quaterdecies del D.Lgs. 196/2003 e ss.mm.ii.) del Titolare ha il compito di:

- dare attuazione alle linee guida fornite dal Titolare in materia di trattamento dei dati personali;
- identificare e implementare, avvalendosi della struttura organizzativa aziendale e di eventuali consulenti, ogni attività che sia finalizzata a conseguire la conformità dell'operato in materia di protezione dei dati personali alle disposizioni vigenti, con particolare riguardo all'art. 5 del Regolamento in cui sono definiti i principi di liceità, correttezza e trasparenza, limitazione delle finalità, minimizzazione dei dati, esattezza, limitazione dei tempi di conservazione, integrità e riservatezza, responsabilizzazione;
- attivarsi per istituire il Modello Organizzativo “Data Protection” per la protezione dei dati personali individuando ruoli, competenze e funzioni previste, in linea con la normativa per quanto agli

ambiti di competenza. In particolare, tra l'altro, egli dovrà provvedere alla nomina delle seguenti figure:

- o I soggetti Autorizzati al trattamento ai sensi dell'art. 29 del GDPR;
- o Le ulteriori funzioni previste dal Modello Organizzativo "Data Protection, quali, consulente privacy (Privacy Officer), Amministratore di Sistema (AdS), Referente privacy, etc.
- attivarsi per nominare quali Responsabili del Trattamento, ai sensi dell'art. 28 del GDPR, i fornitori di servizi (outsourcers) a cui la Società, quale Titolare del Trattamento, ricorre per l'effettuazione di trattamenti di dati personali, provvedendo alla valutazione dei requisiti e delle garanzie in capo agli stessi outsourcers e adottando tutto quanto necessario per la piena conformità al Regolamento in generale e all'art. 28 dello stesso, in particolare;
- adottare ogni soluzione organizzativa idonea ad assicurare che il Responsabile della Protezione dei Dati (RDP/DPO) sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali;
- attivarsi al fine di fornire ai soggetti interni od esterni all'organizzazione del Titolare il necessario supporto per l'esecuzione di quanto previsto da contratti e mansionari nel rispetto delle istruzioni di cui al punto precedente e per la soluzione di problematiche inerenti al trattamento dei dati personali;
- vigilare sull'operato dei soggetti interni od esterni all'organizzazione, accertando che si conformino alle istruzioni formulate, e - su richiesta della Società - fornire un report sullo stato di conformità alla normativa vigente per quanto di sua competenza;
- verificare, in concerto con il/DPO, che gli Autorizzati abbiano ricevuto una formazione adeguata;
- attivarsi al fine di adempiere agli obblighi di informativa e raccolta e gestione dei consensi, individuando i casi in cui sia necessario che la Società predisponga nuovi modelli di informativa;
- attivarsi affinché la Società si conformi agli obblighi attinenti alla sicurezza dei dati personali e dei trattamenti di cui agli artt. 24 e 25 del Regolamento, curando in particolare che siano osservati i principi di protezione dei dati fin dalla progettazione e protezione per impostazione predefinita;
- attivarsi affinché la Società possa dimostrare di essere conforme alle disposizioni normative contribuendo, ove richiesto, alla compilazione del Registro dei trattamenti, alla valutazione dei rischi e al riscontro dei Diritti degli Interessati (ex artt. 15 e ss del GDPR);
- adottare le necessarie procedure o modalità operative per l'efficace gestione degli obblighi di notifica di violazione di cui agli artt. 33 e 34 del Regolamento e in ipotesi di accertate violazioni, col supporto del RPD che sovrintenderà il processo di valutazione dell'incidente anche al fine di fornire le informazioni utili a determinare:
 - o la valutazione della gravità dei rischi conseguenti;
 - o la valutazione dell'eventuale necessità di notificare l'autorità entro i termini di legge (72 ore);
 - o la valutazione dell'eventuale necessità di comunicazione agli interessati (art. 34 GDPR);
 - o la redazione del contenuto e la scelta delle modalità di trasmissione delle citate notificazione e comunicazione.

- nei casi previsti dal Regolamento, individuare i tipi di trattamento che possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche ed eseguire l'iter di valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali;
- adottare quanto necessario, anche ai sensi degli artt. 44 e ss. del GDPR, affinché gli eventuali trasferimenti di dati personali verso Paesi extra UE avvengano nel rispetto delle disposizioni del Regolamento;
- svolgere un ruolo di coordinamento tra i Soggetti interni che compongono l'Assetto Organizzativo Data Protection e il RPD/DPO;
- gestire direttamente, di concerto con il Responsabile della Protezione dei Dati Personali (DPO), i rapporti con il Garante per la protezione dei dati personali e le altre Autorità Pubbliche relativamente alle questioni inerenti al Regolamento.
- adempiere ad ogni altro obbligo prescritto dal Regolamento e dai provvedimenti emanati dall'Autorità Garante in capo al Titolare del Trattamento, se rientrante nei suoi poteri gerarchici, organizzativi e di spesa. Nei casi in cui non vi possa adempiere, per carenze organizzative, difficoltà operative o di altri generi, carenza di budget o eccedente i propri limiti di spesa o qualsiasi altra ragione, il Delegato del Titolare dovrà informare tempestivamente il delegante, fornendo ogni supporto operativo per la migliore gestione dell'obbligo;
- Fornire, su richiesta, un report sullo stato di conformità della Società alla normativa vigente in materia di protezione dei dati personali, evidenziando eventuali non conformità e criticità.

Referenti Data Protection (se nominati)

Considerata la struttura e i trattamenti di dati personali effettuati dalla società, nella sua funzione di Titolare dei trattamenti che effettua, può nominare dei "Referenti Data Protection" che lo affianchino e coadiuvano al fine di garantire il pieno rispetto dei principi e delle disposizioni di cui al GDPR.

La designazione di un Referente Privacy non appare incompatibile con il dettato del GDPR, in particolare con riferimento a strutture di particolare complessità ove risulta opportuno definire una struttura organizzativa Data Protection adeguata che permetta di stabilire in modo puntuale i ruoli e le responsabilità dei soggetti che trattano i dati personali.

Ciò posto, il Referente deve essere individuato e nominato, con apposito atto, dal Titolare (o dal Designato), tenuto conto del ruolo, delle mansioni e delle relative responsabilità attribuite al dipendente sulla base del contratto di lavoro in essere tra lo stesso e il Titolare, in ragione delle competenze dimostrate in termini di affidabilità, esperienza e capacità nello svolgimento dei compiti. In tale contesto, il Referente si impegnerà ad adempiere alle istruzioni descritte nell'atto di nomina.

I Referenti Data Protection devono assicurare che chiunque sia sottoposto alla loro supervisione e coordinamento osservi quanto previsto all'interno del Modello di Data Protection della Società e la normativa vigente, ivi incluse le direttive delle Autorità competenti in materia di dati personali. I Referenti assicurano altresì il raggiungimento e il mantenimento di un livello di protezione adeguato in relazione allo specifico o agli specifici trattamenti di dati personali.

Con riferimento alla gestione degli aspetti "organizzativo-gestionali" i Referenti devono garantire:

- la proposizione al Delegato del Titolare nell'organizzazione delle prestazioni e dei servizi che comportano il trattamento di Dati Personali;

- l’implementazione delle idonee misure organizzative identificate dal Titolare per quanto di propria competenza;
- la propria collaborazione nella applicazione delle previste misure di Accountability previste dalla normativa.
- il monitoraggio del livello di adeguatezza delle misure organizzative identificate e implementate (art. 32 GDPR);
- la correttezza, l’esattezza e la completezza di dati personali oggetto di trattamento presso la società;
- l’avvenuta nomina con atto formale delle persone Autorizzate al trattamento dei dati personali e che possono avere accesso agli stessi;
- che non siano trasmesse e non sia consentito l’accesso ai Dati Personali a soggetti non Autorizzati del loro trattamento;
- supporto alla gestione del processo per le violazioni di dati personali, definito dal Delegato del Titolare, e in ipotesi di accertate violazioni, col supporto del consulente privacy e del RPD, partecipare al processo di valutazione dell’incidente anche al fine di fornire al Delegato del Titolare le informazioni utili a determinare:
 - o la valutazione della gravità dei rischi conseguenti;
 - o la valutazione dell’eventuale necessità di notificare l’autorità entro i termini di legge (72 ore);
 - o la valutazione dell’eventuale necessità di comunicazione agli interessati (art. 34 GDPR);
 - o la redazione del contenuto e la scelta delle modalità di trasmissione delle citate notificazione e comunicazione.

Autorizzato al trattamento

La società, in qualità di Titolare, ravvisa la necessità di individuare i soggetti interni da autorizzare a compiere operazioni di trattamento di dati personali contenuti in banche dati elettroniche e/o cartacee. Ai sensi della normativa vigente, tali soggetti sono designati “Autorizzati”, ovvero “le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare del trattamento”.

Pertanto, in ottemperanza a quanto previsto dalle disposizioni normative, ogni dipendente o collaboratore del Titolare che, per le mansioni assegnate, debba trattare dati personali, deve essere designato per iscritto mediante una lettera di conferimento dell’incarico al trattamento dei dati personali, con la specificazione dei compiti affidati in materia di trattamento dati personali, anche per gruppi omogenei di lavoro, dei compiti che gli sono affidati, nonché delle banche dati cui avrà accesso nello svolgimento delle proprie mansioni.

Al momento dell’assunzione di nuovo personale addetto alle funzioni preposte al trattamento dei dati personali, l’Area PERSONALE provvede alla consegna della relativa lettera di designazione ad “Autorizzato”. Eventuali variazioni alle lettere di designazione sono di competenza dell’Area PERSONALE.

Amministratore di Sistema (AdS, se nominato)

La società identifica con il ruolo di “Amministratore di Sistema” la figura professionale preposta alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, quali amministratori di banche dati, amministratori di rete e di apparati di sicurezza, amministratori di sistemi software. Tali soggetti, nelle proprie consuete attività, sono in molti casi concretamente responsabili di fasi operative che possono comportare elevate criticità rispetto alla protezione dei dati personali.

Il Titolare o il delegato del Titolare del trattamento dei dati designano individualmente l’AdS secondo un preciso profilo di autorizzazione. La lettera di incarico all’Amministratore di sistema dovrà contenere: - l’attestazione che l’Ads ha le caratteristiche richieste dalla legge.

La nomina ad Amministratore di Sistema è effettuata previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

La designazione deve, altresì, essere individuale e recare l’elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato. Inoltre, nel caso di servizi di amministrazione di sistema affidati in outsourcing, la funzione Information Technology deve conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali Amministratori di Sistema.

I compiti dell’Amministratore di sistema consistono nel:

- a) gestire, nel rispetto delle misure di sicurezza applicate dalla Società, il sistema informatico in cui risiedono le banche dati della Società;
- b) monitorare il sistema di sicurezza informatico (idoneo a rispettare le prescrizioni dell’art. 32 del GDPR) adottato dalla Società, adeguandolo anche alle eventuali e future norme in materia di sicurezza;
- c) assegnare e gestire il sistema di autenticazione informatica secondo le modalità ritenute idonee dalla Società e quindi, fra le altre, generare, sostituire ed invalidare, in relazione agli strumenti e alle applicazioni informatiche utilizzate, le parole chiave ed i Codici identificativi personali da assegnare agli autorizzati al trattamento dati;
- d) procedere alla disattivazione dei Codici identificativi personali, in caso di perdita della qualità che consentiva all’utente o autorizzato l’accesso all’elaboratore, oppure nel caso di mancato utilizzo dei Codici identificativi personali per oltre 6 (sei) mesi;
- e) collaborare con la Società per l’attuazione delle prescrizioni impartite dall’Autorità Garante e comunicare prontamente alla Società medesima qualsiasi situazione che possa compromettere il corretto trattamento informatico dei dati personali.

L’operato dell’Amministratore di Sistema deve essere oggetto di supervisione da parte del Delegato del Titolare, e con cadenza almeno annuale tesa a controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalla normativa applicabile in materia di protezione dei dati personali.

Responsabile della Protezione dei Dati (RPD) - DPO Data Protection Officer

Criteria di selezione

Nell'individuare il soggetto più idoneo a ricoprire il ruolo di RPD, la società, in quanto Titolare deve tenere in considerazione le indicazioni previste dal GDPR e le linee guida emanate dal WP29 prima e dall'EDPB ora, e dal Garante.

Il Titolare deve accertare che il soggetto individuato come RPD non sia tra coloro che svolgono un ruolo che comporta la definizione delle finalità o modalità del trattamento dei dati personali, in quanto ciò determinerebbe una situazione di conflitto d'interessi e, quindi, una violazione del requisito dell'indipendenza.

A tal fine, si ritengono senz'altro in conflitto d'interessi le seguenti posizioni di management di alto livello: Direttore Generale, responsabile operativo, finanziario, IT, non escludendo comunque a priori che conflitti si possano determinare anche con posizioni diverse, anche di livello e funzioni inferiori, nonché in caso di RPD di nomina esterna.

Individuazione

La Società ha optato per designare una RPD/DPO (esterno), in forza di un contratto di servizi, che possiede le seguenti caratteristiche:

- conoscenza specialistica della normativa e della prassi in materia di protezione dei dati personali;
- capacità di adempiere ai compiti di cui sarà responsabile come RPD, anche in termini di esperienza nel settore del business della Società;
- caratteristiche personali di integrità ed etica professionale;
- assenza di situazioni di conflitto di interesse.

Designazione

La Società designa il RPD con apposito atto di nomina disciplinante l'attribuzione dei relativi compiti, poteri, durata, cessazione del rapporto e responsabilità.

La Società, inoltre, deve assicurarsi che siano adottate misure idonee a garantire che il RPD:

- possa usufruire di adeguate infrastrutture e risorse umane e finanziarie, nonché, a seconda delle eventuali ulteriori funzioni svolte dal soggetto di volta in volta designato, di tempo sufficiente per l'espletamento dei suoi compiti. Le infrastrutture e le risorse attribuite al RPD ed al suo eventuale Team devono essere rivalutate con cadenza annuale alla luce della complessità e/o sensibilità dei trattamenti effettuati dalla società;
- abbia una posizione tale da poter interagire direttamente con i vertici gerarchici della Società e, se consulente esterno, gli sia garantita la possibilità di avere un contatto diretto con gli stessi;
- non riceva alcuna istruzione per l'esecuzione dei suoi compiti;
- non sia rimosso o penalizzato professionalmente in conseguenza dello svolgimento dei suoi compiti;

- abbia accesso ai dati personali e ai trattamenti effettuati dalla società, al fine di mantenere la propria conoscenza specialistica dell'organizzazione privacy della Società;
- se dipendente, sia messo nella condizione di poter curare il proprio aggiornamento in materia di protezione dei dati personali, partecipando ad appositi corsi di formazione che accrescano di continuo il livello delle proprie competenze.

Una volta designato il RPD, la Società deve provvedere a:

- a) comunicare ufficialmente la nomina a tutto il personale, in modo da garantire che il ruolo e le funzioni del RPD siano note a tutta la società;
- b) pubblicarne i dati di contatto, in modo che questi siano accessibili da parte degli Interessati (a titolo esemplificativo e non esaustivo: sul sito Internet e sulle informative rese agli interessati);
- c) comunicare i dati di contatto all'Autorità di Controllo.

Con specifico riferimento a quanto previsto alle precedenti lettere b) e c), i dati di contatto del RPD dovrebbero comprendere tutte quelle informazioni che consentono agli interessati e all'autorità di controllo di raggiungere facilmente il RPD (i.e. recapito postale e/o indirizzo E-mail/PEC).

Compiti e Responsabilità

Il RPD è tenuto ad assolvere gli obblighi enucleati dall'art. 39 del GDPR e di seguito indicati:

- a) informare e fornire consulenza al Titolare nonché ai dipendenti in merito agli obblighi derivanti dal Regolamento e da altre disposizioni relative alla protezione dei dati;
- b) sorvegliare l'osservanza del Regolamento, e della normativa privacy in generale, nonché delle politiche del Titolare in materia di protezione dei dati, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle attività di controllo connesse;
- c) fornire, qualora fosse richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
- d) cooperare con l'autorità di controllo;
- e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, ed effettuare consultazioni relativamente a qualunque altra questione, e, per gli interessati, anche in merito all'esercizio dei diritti ad essi attribuiti dal Regolamento.

Fermo restando quanto sopra, il RPD riferisce direttamente al vertice gerarchico della Società ogni problematica, violazione ed esigenza, rispettando il segreto e la riservatezza in merito all'adempimento dei propri compiti.

Inoltre, al fine di consentire al RPD di svolgere i compiti sopra elencati, la società deve attuare tutte le misure idonee a far sì che esso sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali e, in particolare, garantire che:

- in ottemperanza al principio di privacy by design di cui all'art.25 del GDPR, il RPD sia invitato a partecipare su base regolare alle riunioni del Management di alto e medio livello e sia coinvolto in ogni occasione in cui siano assunte decisioni che impattano sulla protezione dei dati personali;
- i pareri espressi dal RPD ricevano sempre la dovuta considerazione. Laddove si dovesse verificare una circostanza che determina un disaccordo tra il Delegato del Titolare la posizione del RPD,

la società deve documentare le motivazioni che hanno portato all'adozione della condotta difforme da quella raccomandata dal RPD;

- il RPD sia tempestivamente informato e consultato nell'eventualità in cui si verifichi una violazione dei dati o altro incidente avente ad oggetto gli stessi.

Nello svolgimento dei compiti sopra indicati, il RPD deve adottare un approccio basato sul rischio, definendo sempre un ordine di priorità delle attività da svolgersi e concentrandosi sulle questioni che presentino maggiori rischi per protezione dei dati. Fermo restando ciò, il RPD non deve in ogni caso mancare di sorvegliare il grado di conformità anche dei trattamenti associati ad un livello di rischio comparativamente inferiore.

Responsabile del Trattamento

La Società, in qualità di Titolare, per effetto della conclusione ed esecuzione di specifici contratti, ha demandato alcuni servizi che prevedono il trattamento di dati personali in sua titolarità a soggetti esterni alla propria struttura. In tali casi, i soggetti esterni sono nominati Responsabili del Trattamento, intesi, ai sensi dell'art. 4 del GDPR, come "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento".

Il Responsabile del trattamento deve essere nominato, con apposito contratto o atto giuridico, dal Titolare del Trattamento o dal suo Delegato, in considerazione delle esigenze manifestate dalle singole (Aree, Direzioni, Servizi) in merito alla necessità di esternalizzare alcuni servizi che prevedono il trattamento di dati personali.

Secondo la normativa vigente, il Responsabile è tenuto a presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato.

Il Responsabile, inoltre, non può ricorrere ad un altro Responsabile senza previa autorizzazione scritta, specifica o generale, della Società. In caso di autorizzazione, il Responsabile esterno è tenuto a nominare il subfornitore Responsabile del trattamento e ad imporre allo stesso, tramite contratto o atto giuridico, i medesimi doveri in materia di protezione dei dati personali che il Titolare gli ha prescritto.

I trattamenti da parte di un Responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norme del diritto dell'Unione o degli Stati membri; tale contratto tra la Società ed il Responsabile del trattamento, oltre a vincolare a vicenda le due figure, deve prevedere la materia disciplinata, la durata del trattamento, la natura e le finalità del trattamento nonché il tipo di dati personali e le categorie di interessati a cui gli stessi dati si riferiscono.

Il GDPR prevede una serie di condizioni in rapporto ai criteri di selezione, individuazione e nomina del Responsabile esterno, come trattato in dettaglio nel successivo "Processo di nomina del Responsabile esterno del trattamento".

Processo di nomina del responsabile esterno del trattamento

Il ruolo di Responsabile del trattamento dei dati è attribuito ai SOGGETTI ESTERNI alla società cui vengono delegate attività di competenza della Società o che svolgono attività connesse, strumentali e di

supporto, ivi incluse le attività manutentive, che comportano l'uso di dati personali, comuni e/o sensibili di cui la società è Titolare e/o Responsabile.

Ogniqualvolta un trattamento di dati personali sia effettuato per conto della Società da parte di un soggetto terzo, il richiedente il servizio che sarà effettuato dal terzo attraverso il trattamento di dati personali è tenuto a dare comunicazione, senza ritardo, alla funzione competente degli acquisti fornendo indicazione circa la tipologia dei dati trattati e le finalità del trattamento.

A tali soggetti saranno applicate le politiche di tutela dei dati personali previste nel “Modello di Organizzazione dei dati personali” adottato dalla Società; nel caso in cui il Referente Data Protection intende operare delle deroghe a tali misure dovrà condividere la deroga proposta con il Delegato al Trattamento - che si attiverà per svolgere le necessarie valutazioni. In ogni caso tutte le deroghe alle politiche di tutela dei dati personali previste nel “MOP” per quanto attiene i Responsabili devono essere comunicate tempestivamente al RPD.

Nel caso di trattamento di dati personali effettuato per conto della Società da parte di un soggetto terzo, tale trattamento sarà disciplinato da un apposito contratto che vincoli il terzo agli obblighi ed alle istruzioni fornite.

Il contratto o altro atto giuridico deve prevedere, in particolare, che il Responsabile:

- tratti i dati personali soltanto su istruzione documentata del Titolare e/o del Responsabile, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il Titolare e/o il Responsabile circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
- garantisca che le persone Autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- adotti tutte le misure di sicurezza richieste ai sensi dell'articolo 32 del GDPR;
- rispetti le condizioni di cui ai par. 2 e 4, art.28 del GDPR per ricorrere a un altro Responsabile del trattamento;
- tenendo conto della natura del trattamento, assista la Società con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare e/o del Responsabile di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
- assista il Titolare e/o il Responsabile nel garantire il rispetto degli obblighi di cui agli artt. 32 - 36 del GDPR, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
- su scelta del Titolare e/o del Responsabile, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;

- metta a disposizione del Titolare e/o del Responsabile tutte le informazioni necessarie e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzate dal Titolare e/o del Responsabile del trattamento o da un altro soggetto da questi Incaricato;
- sia obbligato ad informare immediatamente il Titolare e/o Responsabile del trattamento qualora a suo parere una istruzione violi il GDPR o altre disposizioni nazionali o dell'Unione relative alla protezione dei dati.

Tale contratto può, altresì, prevedere il diritto della Società di risolvere il contratto stesso in caso di inadempimento da parte del soggetto designato agli obblighi previsti in forza dell'atto di nomina.

La società effettua una verifica sull'operato dei Responsabili del trattamento, al fine di monitorare il rispetto della normativa in materia di protezione dei dati personali e delle istruzioni impartite.

Consulente Privacy / Privacy Officer (se presente)

Criteri di selezione

Il Designato deve accertare che il soggetto individuato abbia esperienza, capacità ed affidabilità fornendo idonee garanzie del pieno rispetto delle vigenti disposizioni in materia di trattamento. I requisiti, invero, sono da valutare alla luce dell'idoneità, della predisposizione e dell'inclinazione del soggetto a coadiuvare il Titolare negli adempimenti di legge e ad assecondarne e/o svilupparne le strategie relative alla finalità e modalità dei trattamenti ed alla messa in sicurezza dei dati.

Individuazione

La Società che ha optato per designare una Consulente Privacy (esterno), in forza di un contratto di servizi, che possiede le seguenti caratteristiche:

- conoscenza specialistica della normativa e della prassi in materia di protezione dei dati personali;
- caratteristiche personali di integrità ed etica professionale;
- assenza di situazioni di conflitto di interesse.

Compiti e Responsabilità

Il Privacy Officer agisce sotto la diretta supervisione del Designato del Titolare e dovrà:

- aggiornare le informative verso gli interessati;
- supportare le funzioni della società nelle nomine verso autorizzati, Responsabili del trattamento, altre funzioni;
- supportare l'Amministratore di Sistema nell'applicazione del provvedimento a suo carico;
- supportare le funzioni della società nell'applicazione di specifici provvedimenti emessi dal Garante;
- partecipare a riunioni ogni qualvolta si introduca all'interno della società una nuova tecnologia o debbano essere attuate campagne o operazioni che riguardino il trattamento dei dati personali e impostare unitamente al delegato del trattamento la valutazione preventiva di impatto del rischio;

- partecipare a riunioni ogni qualvolta si introducano nuove misure sulla sicurezza o potenziali sistemi di controllo a distanza dei dipendenti o qualora si vogliano applicare politiche della società che impattano sulla riservatezza dei dipendenti;
- predisporre e mantenere insieme al Designato la documentazione richiesta dal GDPR;
- mettere in atto le disposizioni richieste dal RDP/DPO in materia di protezione dei dati;
- relazionare sullo stato di avanzamento ed eventuali problematiche;
- supportare il DPO nel predisporre e tenere sotto controllo il piano delle attività previste e nel pianificare e condurre o sorvegliare la conduzione di attività di audit (sia di conformità al GDPR che relativi all'applicazione delle procedure interne che impattano sul GDPR);
- tenere sotto controllo lo stato di avanzamento delle eventuali criticità emerse nel corso dell'Audit;
- supportare il DPO nel tenere sotto controllo lo stato di avanzamento delle misure pianificate per la mitigazione dei rischi;

PRINCIPI GENERALI PER IL TRATTAMENTO DEI DATI

Trattamento di dati personali e condizioni di liceità

Ai sensi dell'art.4 del Regolamento, con l'espressione "trattamento di dati personali" s'intende "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", in particolare:

- la raccolta dei dati;
- la registrazione dei dati, ovvero il loro inserimento su supporti, automatizzati o manuali, al fine di rendere i dati disponibili per successivi trattamenti;
- l'organizzazione dei dati in senso stretto, ovvero il permesso di lavorazione che ne favorisca la fruibilità attraverso l'aggregazione o la disaggregazione, l'accorpamento, la catalogazione, etc.;
- la conservazione dei dati alla quale la legge dedica particolari attenzioni sotto il profilo della sicurezza;
- l'adattamento o la modifica dei dati registrati in relazione a variazioni o a nuove acquisizioni;
- l'estrazione, ipotesi specifica che rientra nell'ipotesi più generale dell'elaborazione;
- la consultazione;
- l'uso;
- la comunicazione, ovvero la trasmissione dei dati ad uno o più soggetti determinati, in qualunque forma, mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione;
- il raffronto o l'interconnessione, ovvero la messa in relazione di banche dati diverse e distinte fra loro al fine di compiere ulteriori processi di elaborazione, selezione, estrazione o raffronto;
- la limitazione;
- la cancellazione;
- la distruzione.

Il trattamento di dati personali è esercitabile solo da parte dei soggetti individuati da parte del Titolare; non è consentito il trattamento da parte di persone non autorizzate. Il trattamento dei dati, anche di natura sensibile o giudiziaria, effettuato dalla Società è diretto all'espletamento delle finalità strettamente connesse all'attività ed i servizi erogati. La Società tratta, inoltre, i dati, anche di natura sensibile dei propri dipendenti per le finalità di instaurazione e di gestione dei rapporti di lavoro.

I dati personali oggetto del trattamento, come previsto dall'art.5 del GDPR, devono essere:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza");
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità ("limitazione delle finalità");
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati");
- esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati ("esattezza");

- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (“limitazione della conservazione”);
- trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

La Società è competente per il rispetto dei principi sopra elencati e devono essere in grado di dimostrarlo. Come sancito dall'art.6 del Regolamento, 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.

Privacy by design e Privacy by default

L'articolo 25 del GDPR pone l'obbligo per la Società di:

- mettere in atto misure tecniche ed organizzative adeguate a proteggere i dati personali sia al momento della determinazione dei mezzi di trattamento sia all'atto di trattamento stesso (i.e. principio di “**Privacy by Design**”) e volte ad attuare in modo efficace i principi di protezione dei dati e a integrare nel trattamento le necessarie garanzie al fine di tutelare i diritti degli interessati;
- mettere in atto misure tecniche ed organizzative idonee a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari al perseguimento delle specifiche finalità per cui sono raccolti e per il periodo strettamente necessario a tale fine (i.e. principio di “**Privacy by Default**”)

La Società riconosce e promuove il valore e i benefici di un approccio proattivo all'adozione di prassi e tecniche di tutela dei dati personali degli interessati, a partire dalla fase di “design di nuove iniziative di business e/o di sistemi”, in maniera consistente su tutti i programmi e progetti intrapresi.

A tal fine, il Designato deve considerare la tutela dei diritti e delle libertà degli interessati quale requisito fondamentale nello sviluppo di nuovi prodotti e/o servizi, riconoscendo i potenziali rischi e le limitazioni che potrebbero derivare per tali diritti e libertà.

In particolare, nello sviluppo di qualsivoglia nuovo servizio che abbia ad oggetto un trattamento dei dati personali, o nell'ipotesi di modifiche di servizi già realizzati o resi della Società o di cambiamenti significativi nelle modalità di progettazione ed erogazione di tali servizi, nonché in tutte le occasioni in cui il Designato, coadiuvato dai Referenti Data Protection (nel caso in cui siano nominati) intenda procedere con iniziative di qualsivoglia natura che abbiano come destinatari utenti della Società, dipendenti, fornitori o altre categorie di interessati, questi devono immediatamente coinvolgere nel progetto il DPO, assicurandosi che siano tempestivamente messe a disposizione tutte le informazioni pertinenti al potenziale trattamento, possa compiutamente valutare gli impatti che potrebbero derivare agli interessati a seguito del trattamento dei dati e coinvolgere il Designato per le opportune valutazioni.

Principio di minimizzazione

Gli Autorizzati dovranno attenersi al principio di minimizzazione dei dati, in forza del quale non dovranno essere richiesti agli interessati o, più in generale, non dovranno essere trattati dati personali ulteriori o eccedenti rispetto a quelli strettamente necessari al perseguimento delle finalità di trattamento.

Periodo di conservazione dei dati personali

I dati personali raccolti non devono essere trattati per un periodo eccedente quello strettamente necessario per il raggiungimento delle finalità perseguite dalla Società.

Pertanto, al fine di ottemperare ai principi di “Privacy by Design” e “Privacy by Default”, il Designato, coadiuvato dai Referenti Data Protection (nel caso in cui siano nominati), fin dalla fase progettuale del servizio e/o iniziativa devono svolgere specifiche valutazioni sulla durata del trattamento e relativo periodo di conservazione dei dati personali, anche in virtù di eventuali obblighi di legge.

Sulla base delle risultanze della valutazione svolta, devono essere identificati appositi presidi e processi volti a garantire che i dati personali non vengano trattati e conservati per un periodo superiore a quello strettamente necessario al perseguimento delle finalità previste, salvo l'adempimento di specifici obblighi di conservazione imposti dalla legge.

Accesso ai dati personali

Nello sviluppo del servizio il Designato, coadiuvato dai Referenti Data Protection (nel caso in cui siano nominati) dovrà mettere in atto misure tecniche ed organizzative idonee ad assicurare che, per impostazione predefinita, i dati personali non siano resi accessibili ad un numero indefinito di persone e che, al contrario, l'accessibilità agli stessi sia segregata sulla base del principio di necessità. In tal senso, l'accesso dovrà essere reso disponibile esclusivamente a quei soggetti che sono tenuti al trattamento di quei dati personali per il raggiungimento delle finalità perseguite dalla società.

Misure di sicurezza

Il Designato, coadiuvato dai Referenti Data Protection (nel caso in cui siano nominati) deve valutare le misure di sicurezza logiche o fisiche da applicare al trattamento, al fine di assicurare che, per impostazione predefinita, siano implementate le più stringenti possibili, individuando specifici presidi volti a prevenire eventi di violazione interni o esterni alla Società.

Al fine di assicurare un'efficace protezione dei dati personali degli interessati su tutta la filiera di elaborazione e conservazione, la società deve dotarsi di tecnologie di sicurezza all'avanguardia, non limitandosi a salvaguardare la confidenzialità, l'integrità e la disponibilità delle informazioni per tutto il periodo di durata del trattamento, ma anche assicurando la loro eliminazione sicura o in alternativa la loro anonimizzazione irreversibile, al termine dello stesso, o in seguito a richieste degli interessati, nel rispetto dei diritti all'oblio e alla limitazione.

Sulla base dei suddetti principi, tutte le nuove iniziative di business che prevedono il trattamento di dati personali devono essere valutate con attenzione dal Designato, coadiuvato dai Referenti Data Protection (nel caso in cui siano nominati) competenti, chiedendo l'eventuale consulenza del RPD della Società, utilizzando criteri appropriati al grado di sensibilità dei dati stessi e tenendo sempre in considerazione il punto di vista degli interessati, ad esempio la propensione o la reticenza alla condivisione delle informazioni riguardanti la propria sfera personale, al fine di garantirne il rispetto.

Trasferimento di dati personali all'estero

Come sancito dall'art.44 del Regolamento “qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, ha luogo soltanto se il Titolare del trattamento e il Responsabile del trattamento rispettano le condizioni di cui al presente capo, fatte salve le altre disposizioni del presente regolamento.”

In particolare, la Società deve tenere in considerazione che il trasferimento - a soggetti stabiliti fuori dall'Unione Europea - di dati personali di cui essi sono Titolari richiede, alternativamente, la sussistenza di almeno una delle seguenti condizioni:

- I. il trasferimento verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione Europea ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato;
- II. nel caso in cui non siano state emanate decisioni di adeguatezza, il trasferimento dei dati personali deve essere effettuato sulla base di accordi contrattuali, stipulati tra la società ed i soggetti destinatari dei dati stabiliti fuori dall'Unione Europea (Es.: Responsabili “esterni”), che forniscano garanzie adeguate agli utenti (ad esempio l'esercizio da parte di questi dei diritti a loro accordati dal GDPR).

I DIRITTI DELL'INTERESSATO

Ai sensi della normativa vigente, l'interessato gode del diritto di:

- **ricevere un'informativa** contenente i seguenti elementi:
 - identità e dati di contatto del Titolare;
 - dati di contatto del RPD della Società (se nominato);
 - finalità di trattamento cui sono destinati i dati personali, nonché la base giuridica del trattamento;
 - ove applicabile, i legittimi interessi perseguiti dal Titolare o da terzi;
 - i destinatari o le categorie di destinatari dei dati personali;
 - l'intenzione del Titolare di trasferire i dati personali ad un paese terzo o a un'organizzazione internazionale;
 - il periodo di conservazione dei dati personali o, se non è possibile, i criteri utilizzati per determinare tale periodo;
 - la possibilità di esercitare i diritti riconosciuti all'interessato, ivi inclusi il diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento e il diritto di proporre reclamo all'Autorità di Controllo;
 - la natura obbligatoria o facoltativa del conferimento dei dati;
- **revocare**, in qualsiasi momento, **il consenso**, senza alcun condizionamento e con la stessa facilità con cui è stato prestato;
- **accesso**, consistente nell'ottenere dalla società la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso a tali dati – compresa una copia degli stessi – ed alle informazioni elencate all'articolo 15 GDPR;
- **rettifica**, consistente nella possibilità di ottenere dalla società la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo e/o l'integrazione dei dati personali incompleti;
- **cancellazione** (c.d. diritto all'oblio), consistente nella facoltà di ottenere dalla società la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo nel rispetto delle condizioni della normativa;
- **limitazione di trattamento**, consistente nella possibilità di ottenere dalla società la limitazione (temporanea) del trattamento al ricorrere di una delle seguenti ipotesi:
 - l'interessato contesta l'esattezza dei dati personali;
 - il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali chiedendone che ne sia limitato l'utilizzo;
 - nonostante la finalità di trattamento si sia esaurita, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
 - a seguito dell'esercizio del diritto di opposizione da parte dell'interessato, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi della Società rispetto a quelli dell'interessato;
- **ottenere** la comunicazione da parte della Società a ciascuno dei destinatari cui sono trasmessi i dati personali dell'interessato, di eventuali rettifiche, cancellazioni o limitazioni del trattamento, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato.

- **portabilità dei dati**, consistente nella facoltà – nei soli casi in cui il trattamento si basa sul consenso o su un contratto ed è effettuato con mezzi automatizzati – di ricevere dalla società, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano forniti dall'interessato stesso, nonché la possibilità di trasmetterli ad un altro titolare senza impedimenti. Inoltre, qualora tecnicamente possibile, il diritto alla portabilità dei dati consente di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro;
- **opposizione**, consistente nel diritto di opporsi, alle condizioni e nel rispetto dei limiti previsti dalla normativa, al trattamento dei dati personali che lo riguardano qualora: (i) necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri; (ii) fondato sull'interesse legittimo del titolare; (iii) finalizzato ad attività di marketing diretto; (iv) finalizzato alla ricerca scientifica o storica o con fini statistici;
- **non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato**, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona, salvo quanto previsto dalla normativa.

Nel caso in cui la Società riceva delle richieste dagli interessati in merito all'esercizio dei propri diritti è necessario formalizzare una risposta dettagliata secondo le seguenti modalità:

- in una **forma concisa, trasparente, intelligibile** e con un **linguaggio semplice e chiaro**;
- per **iscritto**, o con **mezzi elettronici** se la richiesta è stata effettuata con mezzi elettronici. Una **risposta orale** è consentita solo su domanda espressa dall'interessato;
- **senza ingiustificato ritardo** e, al più tardi, entro un mese dal ricevimento della richiesta, salva la possibilità di prorogare tale termine di due mesi nei particolari casi previsti e fermo restando l'obbligo di informare comunque l'interessato del ritardo e dei motivi entro un mese dal ricevimento della richiesta. In ogni caso, se non è possibile soddisfare la richiesta entro un mese dal suo ricevimento, è necessario informare l'interessato (i) che non sarà possibile soddisfare la sua richiesta entro tale termine, (ii) sui motivi della proroga e (iii) sulla possibilità di proporre reclamo ad un'autorità di controllo e ricorso giurisdizionale;
- **gratuitamente**. Può essere addebitato un contributo ragionevole, o negata la soddisfazione della richiesta, solo nel caso di richieste manifestamente infondate o eccessive, anche per la loro ripetitività;
- **dopo aver verificato l'identità** dell'interessato, eventualmente anche domandando informazioni aggiuntive.

Sulla base dei suddetti principi, la Società ha definito una procedura che disciplina le modalità di gestione delle richieste di esercizio dei diritti da parte degli interessati.

IL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

L'art. 30 del Regolamento impone a Titolari e Responsabili del trattamento, con limitate eccezioni, di tenere un Registro delle attività di trattamento svolte sotto la propria responsabilità (il "Registro").

Il Garante per la protezione dei dati personali consiglia fortemente a tutti i Titolari del trattamento ed i responsabili, a prescindere dalle dimensioni organizzative, di dotarsi del Registro dei trattamenti, in quanto parte integrante di un sistema di corretta gestione dei dati personali e fondamentale sia ai fini dell'eventuale supervisione da parte del Garante sia in quanto indispensabile per ogni valutazione e analisi del rischio.

I Registri sono tenuti in forma scritta, anche in formato elettronico. Essi devono contenere le seguenti informazioni minime:

- il nome e i dati di contatto del Titolare, di eventuali Contitolari e del Responsabile della Protezione dei Dati (RPD/DPO);
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui all'art.49 del GDPR, la documentazione delle garanzie adeguate;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'art.32 del GDPR.

Il Registro deve essere sempre **mantenuto aggiornato** rispetto alle attività di trattamento concretamente attuate dalla società. In particolare, è responsabilità del Designato, coadiuvato dai Referenti (nel caso nominati) e del Privacy Officer (se presente) aggiornare il registro per quanto di propria competenza.

Nei casi in cui la società è nominata Responsabile del Trattamento compilerà l'apposito Registro dei trattamenti con le seguenti informazioni minime:

- il nome e i dati di contatto del Responsabile o dei responsabili del trattamento, di ogni Titolare del trattamento per conto del quale agisce il Responsabile del trattamento, del Rappresentante del titolare del trattamento o del Responsabile del trattamento e, ove applicabile, del Responsabile della Protezione dei Dati (RPD);
- le categorie dei trattamenti effettuati per conto di ogni Titolare del trattamento;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui all'art.49 del GDPR, la documentazione delle garanzie adeguate;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'art.32 del GDPR.

La Società, in considerazione ha scelto di compilare e tenere un **unico Registro delle attività di trattamento**.

IL RESPONSABILE DEL TRATTAMENTO

Qualora un trattamento debba essere effettuato per conto del Titolare del trattamento, quest'ultimo, ai sensi dell'art. 28 comma 1 del GDPR, 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 richiesti dal GDPR e garantisca la tutela dei diritti dell'interessato.

Le garanzie richieste potranno essere "dimostrate" con l'adesione ad un codice di condotta approvato (ex art. 40 GDPR) o ad un meccanismo di certificazione (ex art. 42 GDPR). In ogni caso il Titolare del trattamento dovrà selezionare il Responsabile a cui affidare il trattamento dei propri dati valutando le informazioni fornite dal Responsabile a "garanzia" della compliance al GDPR o l'esistenza di un concreto processo di adeguamento in atto.

L'art. 28 del Regolamento prevede l'obbligo in capo al Responsabile del trattamento di consentire e contribuire "alle attività di revisione, comprese le ispezioni, realizzate dal titolare del trattamento o da un altro soggetto da questi incaricato".

Il Titolare del trattamento può prevedere un'attività di monitoraggio e controllo periodico del Responsabile, anche attraverso l'invio di apposite "Check List di controllo" elaborate da parte del Delegato, con l'eventuale supporto consulenziale del consulente privacy e/o dell'RPD, volta a verificare la sussistenza dei caratteri di esperienza, capacità ed affidabilità in capo al Responsabile, nonché sull'effettivo svolgimento delle attività e dei compiti affidati e il rispetto da parte dello stesso di tutte le disposizioni normative in materia di sicurezza dei dati.

Nell'ambito di tale "Check list di controllo" potrebbe essere richiesto al Responsabile, a titolo esemplificativo, di:

- ✓ aver già provveduto ad individuare la figura del RPD, anche laddove non obbligatorio;
- ✓ aver già istituito un Registro delle attività di trattamento (e in tal caso, dando evidenza delle modalità di redazione, aggiornamento, ecc.);
- ✓ aver adottato "policy" per garantire che gli Autorizzati siano obbligati alla riservatezza o per soddisfare eventuali richieste di esercizio dei diritti degli interessati, per la conservazione dei dati o ancora per la gestione delle eventuali violazioni (Data Breach);
- ✓ aver implementato determinate misure di sicurezza, tecniche o organizzative, valutate adeguate a garantire che il trattamento sia conforme al GDPR.

Nei casi di "nuovi" fornitori ai quali sono affidati trattamenti di particolare rilevanza (es.: fornitori software, ecc.) il Titolare valuta l'adeguatezza delle garanzie sufficienti da parte del Responsabile preliminarmente l'affidamento dell'incarico.

Al Responsabile del trattamento potrà essere richiesto di inviare una relazione annuale sullo stato di attuazione della normativa, evidenziando gli aspetti problematici e le difficoltà attuative riscontrate durante il periodo di riferimento. In tal caso, allo scopo di approfondire e/o risolvere aspetti anomali o particolari emersi all'interno della relazione, il Delegato, eventualmente con il supporto consulenziale del consulente privacy e/o dell'RPD, se nominato, si riserverà il diritto di effettuare una visita ispettiva presso il Responsabile del trattamento.

Ai sensi di quanto previsto dall'art. 28 comma 2 del GDPR, il Responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del Titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il Titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al Titolare l'opportunità di opporsi a tali modifiche.

In relazione alle autorizzazioni rilasciate dal Titolare al Responsabile, il Delegato dovrà monitorare se il Responsabile ha nominato "sub-responsabili" e per questi ha riscontrato le stesse garanzie che il Titolare ha richiesto al Responsabile.

INFORMATIVA IN MATERIA DI PROTEZIONE DATI E RICHIESTA DI CONSENSO

L'Informativa in materia di protezione dati

L'Informativa in materia di protezione dati personali è il documento da fornire nel momento in cui vengono raccolti i dati personali dell'interessato. Gli articoli 13 e 14 del GDPR stabiliscono in maniera chiara e dettagliata quelli che sono i contenuti obbligatori che l'Informativa deve contenere.

L'Informativa in materia di protezione dati personali da fornire agli interessati deve essere:

- redatta in maniera trasparente e intelligibile per l'interessato;
- resa disponibile o comunque essere facilmente accessibile;
- scritta in una forma e in un linguaggio semplice e chiaro.

Il rilascio dell'Informativa agli interessati è **adempimento inderogabile**, qualunque sia la base giuridica utilizzata per il trattamento dei dati personali. Il Designato, coadiuvato dai Referenti Data Protection (nel caso in cui siano nominati) deve assicurare che prima dell'acquisizione dei dati personali o contestualmente all'acquisizione degli stessi il processo organizzativo preveda che l'Informativa sia stata consegnata o comunque messa a disposizione degli interessati.

A seconda che i dati siano ottenuti dal Titolare presso il diretto interessato o presso un soggetto terzo, sono previste due differenti tipologie di Informativa: diretta ed indiretta.

L'Informativa diretta

L'art. 13 del GDPR stabilisce che, nel caso in cui la raccolta dei dati personali sia effettuata presso l'interessato, l'Informativa dovrà contenere:

- l'identità e i dati di contatto del Titolare del trattamento;
- i dati di contatto del Responsabile della Protezione dei Dati;
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- se il trattamento si basa su legittimi interessi perseguiti dal Titolare del trattamento o da terzi;
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- 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.
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- 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 dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
- qualora il trattamento si basi sul consenso, l'esistenza del diritto di revocarlo in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca;
- il diritto di proporre reclamo a un'Autorità di controllo;

- 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'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.

Inoltre, qualora il Titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente.

L'Informativa indiretta

Qualora i dati non siano stati ottenuti presso l'interessato, il Titolare prima di avviare il trattamento, deve fornire all'interessato idonea Informativa (ex art. 14 del GDPR) in relazione ai trattamenti effettuati.

In tali casi l'Informativa deve indicare, oltre i contenuti previsti per l'Informativa diretta, anche la fonte da cui sono stati acquisiti i dati personali, specificando il caso in cui i dati provengano da fonti accessibili al pubblico.

Il Titolare del trattamento deve fornire l'Informativa:

- entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;
- nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; oppure
- nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.

La richiesta di consenso

Tra le diverse condizioni che rendono "lecito" il trattamento di dati personali, ai sensi dell'art. 6 par.1 let. a) del GDPR è prevista la richiesta del consenso da parte dell'interessato per una o più specifiche finalità.

L'art. 4 del GDPR definisce il consenso come: "qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento".

Il Regolamento Europeo 679/2016 inoltre richiede l'esplicito consenso nei casi di:

- trattamento di categorie particolari di dati, come dati relativi alla salute o i dati biometrici;
- trasferimento di dati verso paesi terzi o organizzazioni internazionali in assenza di adeguate salvaguardie;
- presenza di processi decisionali automatizzati, inclusa la profilazione.

Il consenso può ritenersi espresso secondo modalità conformi alle condizioni del GDPR, se è:

- **informato**, occorre cioè che l'interessato sia posto in condizioni di conoscere quali dati sono trattati, con che modalità e finalità e i diritti che gli sono attribuiti dalla legge, cioè deve essere rispettato il principio di trasparenza. Inoltre, l'interessato deve essere opportunamente informato sulle conseguenze del suo. L'informazione si ha attraverso l'apposita informativa.
- **Specifico**, cioè relativo alla finalità per la quale è eseguito quel trattamento. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per ogni finalità (Considerando 32 GDPR). Quindi, i dati dovranno essere pertinenti al consenso fornito, e in caso di modifiche del trattamento occorre richiedere un nuovo consenso. Per cui avremo un consenso per il marketing diretto, un consenso per la profilazione, ecc...
- **Libero**, prestato cioè senza condizionamenti e senza dover subire pregiudizi (l'esecuzione di un contratto, compresa la prestazione di un servizio, non deve essere subordinata ad un consenso non necessario per tale esecuzione);
- **Inequivocabile**: deve essere manifestato attraverso una dichiarazione o azione positiva inequivocabile, la richiesta di consenso, laddove inserita nel contesto di una dichiarazione scritta che riguarda anche altre questioni, deve essere chiaramente distinguibile dalle altre materie; non è ammesso il consenso tacito o presunto e non costituiscono valido consenso caselle pre-spuntate su un modulo.

Per quanto riguarda i trattamenti effettuati senza utilizzo di sistemi informatici, il consenso deve essere rilasciato in forma scritta, utilizzando gli appositi moduli e Informativa predisposte dal Titolare e deve riguardare in maniera separata e distinta il trattamento dei dati personali.

Il Titolare deve assicurare la presenza di processi organizzativi che prevedano la conservazione del documento attestante l'avvenuto rilascio del consenso per l'intera durata del trattamento.

**Il consenso per l'accesso ai servizi on-line*

L'accesso ai servizi on-line offerti può essere consentito solo a utenti registrati.

La registrazione deve poter avvenire solo a titolo personale mediante emissione di codici identificativi e chiavi di accesso univoche e può prevedere la conferma mediante procedura che preveda l'invio di una mail all'indirizzo dichiarato nel form/maschera di registrazione dell'interessato con indicazione di un link.

Al fine di garantire una corretta acquisizione del consenso da parte dell'interessato:

- ❖ nessuna delle caselle di "flag" del consenso deve essere preimpostata;
- ❖ l'interessato deve aver selezionato la casella di presa visione dell'Informativa che deve essere distinta da quella per la prestazione del consenso;
- ❖ le caselle di "flag" del consenso devono avere funzione esclusiva e devono essere distinte per ogni trattamento avente finalità diversa;
- ❖ la mancata prestazione del consenso deve impedire l'accesso al servizio on line esclusivamente se è omesso in relazione ai dati che sono necessari all'esecuzione del servizio medesimo.

Il Titolare deve assicurare la presenza di processi automatizzati di tracciatura del consenso prestato dall'Interessato con riferimento alle singole finalità di trattamento

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)

Il GDPR ha introdotto l'obbligo per il Titolare del trattamento di eseguire, al ricorrere di talune condizioni, una Valutazione d'Impatto sulla Protezione dei Dati (Data Protection Impact Assessment, di seguito "DPIA" o semplicemente "Valutazione").

Secondo quanto disposto dall'art. 35, paragrafo 1 del GDPR è previsto in capo al Titolare del trattamento l'onere di procedere ad una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati: "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."

L'effettiva valutazione ed esecuzione della DPIA è in carico al Designato, coadiuvato dai Referenti (se nominati) eventualmente coadiuvati dal supporto del RPD, se nominato, del Consulente Privacy.

Il Designato, coadiuvato dai Referenti Data Protection (nel caso in cui siano nominati) è tenuto a valutare l'obbligatorietà di sottoporre un particolare trattamento a DPIA, al verificarsi di specifiche condizioni. In generale, la DPIA è obbligatoriamente richiesta per i trattamenti che consistono in:

- valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- trattamento, su larga scala, di categorie particolari di dati e relativi a condanne penali e a reati;
- sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Accertata la necessità di svolgere una Valutazione d'Impatto sulla Protezione dei Dati, il Designato coinvolge opportunamente gli altri soggetti interni ed esterni che sono o saranno (in caso di nuovi trattamenti) coinvolti nel trattamento oggetto di DPIA.

L'attività di Valutazione consta dei seguenti step operativi, opportunamente condotti dal Designato:

- identificazione e analisi dei principali rischi per i diritti e le libertà degli interessati in termini di minacce e impatto;
- valutazione del livello di rischio pre e post- identificazione delle contromisure di sicurezza (tecniche e organizzative) atte a mitigare tali rischi.

Nel caso di rischio elevato per i diritti e le libertà degli interessati, nonostante le contromisure di sicurezza identificate, il Designato procede con la consultazione preventiva dell'Autorità di Controllo.

Il RPD monitorerà l'effettiva implementazione delle indicazioni pervenuta dall'Autorità stessa.

Infine, ogniqualvolta vi sia una variazione significativa della natura, delle finalità o delle modalità di trattamento, incluso l'utilizzo di nuove tecnologie, il Designato, coadiuvato dai Referenti Data Protection (nel caso in cui siano nominati) ha la responsabilità di aggiornare la valuDPIA, al fine di monitorarne e stimarne le variazioni in termini di impatto per i diritti e le libertà degli interessati.

I Titolari, in conformità alle prescrizioni normative, si sono dotati di un processo di Valutazione d'Impatto sulla Protezione dei Dati e di una metodologia per l'esecuzione della stessa.

VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

Il GDPR ha introdotto l'obbligo, in capo al Titolare del Trattamento, di notificare all'Autorità di Controllo la violazione dei dati personali, 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 libertà delle persone fisiche cui i dati violati si riferiscono.

Nel caso in cui la suddetta violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del Trattamento deve comunicare la violazione senza ingiustificato ritardo anche agli interessati stessi.

Va inoltre rilevato che, a seconda delle circostanze, una violazione può riguardare la riservatezza, la disponibilità e l'integrità dei dati personali trattati e conservati sia su supporti elettronici sia su supporti fisici (Es.: archiviazione cartacea).

I soggetti interni (Es.: Autorizzati, Amministratori di Sistema, ecc.) autorizzati al trattamento di dati personali, le risorse operanti in ambito IT, nonché i fornitori esterni debitamente designati Responsabili del trattamento possono, nello svolgimento delle attività ad essi demandate, rilevare anomalie o eventi che potrebbero configurarsi come violazioni di dati personali (Data Breach). In tale evenienza, essi sono tenuti a informare tempestivamente il Designato.

A valle della rilevazione / segnalazione di un potenziale Data Breach la Società procede con l'analisi della violazione, al fine di verificarne le categorie di interessati, le categorie di dati compromessi, nonché le altre informazioni necessarie per identificare le contromisure opportune per mitigarne i rischi nonché per eseguire la notifica all'Autorità di Controllo e, laddove necessario, agli interessati.

A titolo esemplificativo e non esaustivo, tali informazioni riguardano:

- Identificabilità degli interessati, ovvero la possibilità che gli interessati possano essere identificati sulla base dei dati oggetto di compromissione;
- Misure di sicurezza attuate, che potrebbero aver mitigato gli impatti derivanti dal Data Breach;
- Numero di individui coinvolti, ovvero la portata in termini numerici degli interessati coinvolti.

Terminata l'analisi del Data Breach occorso la società dovrà:

- ✓ identificare e implementare le azioni di contenimento e risoluzione al fine di mitigare gli impatti della violazione occorsa;
- ✓ valutare l'obbligatorietà di notificare la violazione all'Autorità di Controllo;
- ✓ valutare l'obbligo di notifica agli interessati, nel caso in cui la violazione occorsa presenti rischi elevati per i diritti e le libertà degli interessati.

Laddove necessario, la società effettuerà la notifica all'Autorità di Controllo e ai soggetti interessati con tutte le informazioni previste dalla normativa vigente.

Il Designato, coadiuvato dai Referenti (nel caso in cui siano nominati) e dal Consulente Privacy, è tenuto a predisporre e mantenere un registro interno in cui è documentata qualsiasi violazione dei dati personali, comprese le circostanze, le conseguenze e le misure adottate per porvi rimedio.

Al fine di consentire una gestione efficace e tempestiva delle violazioni di dati personali, la Società si è dotata di un processo di gestione delle situazioni di Data Breach.

FORMAZIONE

L'art. 39, lett. b) del Regolamento prevede espressamente che rientri tra i compiti del RPD “sorvegliare l'osservanza (...) delle politiche del Titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi (...) la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo”.

Inoltre, come sancito dall'art. 32, par.4 della normativa vigente “chiunque abbia accesso a dati personali non tratta tali dati se non istruito in tal senso dal Titolare del trattamento (...)”.

Pertanto, si evince chiaramente che la formazione in materia di Data Protection è considerata un'importante misura di sicurezza per la protezione dei dati personali, che deve essere obbligatoriamente adottata dalla società.

A tal fine, la Società è tenuta ad organizzare interventi di formazione e aggiornamento in materia di tutela della riservatezza e protezione dei dati personali rivolti agli Autorizzati/Designati ed eventualmente a particolari categorie di soggetti esterni autorizzati ai trattamenti di dati personali per conto della Società (Es.: Responsabili del trattamento).

La formazione è finalizzata alla conoscenza delle norme, all'adozione di idonei modelli di comportamento e procedure di trattamento, alla conoscenza delle misure di sicurezza adottate dalla società per il trattamento e la conservazione dei dati, dei rischi individuati e delle modalità per prevenirne i danni.

LE SANZIONI

La mancata applicazione delle disposizioni normative previste dal Regolamento Europeo 679/2016 può prevedere l'irrogazione in capo al Titolare di sanzioni di tipo amministrativo e pecuniario che ai sensi dell'art. 84 del GDPR devono essere effettive, proporzionate e dissuasive. È rimesso alla disciplina dei singoli stati membri dell'Unione Europea definire le norme in materia di sanzioni per violazioni alla normativa in materia di protezione dati personali. In tal senso, le sanzioni connesse alle violazioni amministrative e agli illeciti penali sono state specificate dal Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) n. 2016/679, entrato in vigore il 19 settembre 2018, come modificato dal D.Lgs n. 101 del 10 agosto 2018.

Violazioni da parte del personale della Società

Le norme e i principi di comportamento, nonché le disposizioni procedurali definite dal Titolare in materia di protezione dati personali, hanno carattere vincolante per il personale dipendente della Società, e devono essere considerate aggiuntive rispetto alle norme disciplinari già in vigore presso la Società stessa.

Ogni comportamento in violazione del presente Regolamento può avere importanti ripercussioni per il Titolare e sarà ritenuto grave inosservanza dei doveri del lavoratore. Questo potrà quindi comportare, nei confronti del dipendente inadempiente, l'applicazione di provvedimenti disciplinari, in conformità alle disposizioni di legge e di quanto stabilito nel Regolamento Organico del Personale.

I comportamenti che costituiscono inosservanza del presente Regolamento possono violare, nel contempo, anche disposizioni di legge tali da comportare per il dipendente conseguenze di natura civile e penale. In relazioni a tali condotte anche il Titolare può essere perseguito e sanzionato in conseguenza del comportamento dei propri incaricati.

Violazioni da parte del Responsabile del trattamento

Qualsiasi violazione dei compiti del Responsabile del trattamento costituirà titolo e diritto del Titolare di risoluzione immediata del contratto in essere con il Responsabile, fatta salva in ogni caso, la facoltà del Titolare di richiedere un risarcimento di importo da determinarsi a seconda del livello di rischio e del volume dei dati trattati per ciascun evento che provoca perdita / compromissione dei dati e del loro trattamento protetto durante e dopo l'esecuzione del contratto fondante.

Inoltre, ai sensi dell'art. 82 par. 2 del GDPR, il Responsabile si assumerà la responsabilità nei confronti di chiunque abbia subito un danno dal trattamento effettuato non in conformità agli obblighi del GDPR specificatamente diretti ai Responsabili del trattamento o effettuato in modo difforme o contrario rispetto alle legittime istruzioni del Titolare del trattamento.

In tal senso, il Responsabile si impegnerà a manlevare e tenere indenne il Titolare da qualsiasi pretesa, danno, onere, costo, spesa o pregiudizio di qualsivoglia natura che questa abbia a subire per effetto della violazione - diretta o indiretta - da parte del Responsabile del trattamento.

ALLEGATI

POLITICHE GENERALI PER L'UTILIZZO DI DISPOSITIVI E STRUMENTI INFORMATICI

Titolarità, autorizzazione e finalità di utilizzo degli strumenti informatici

La CARBOSULCIS SPA è titolare dei dispositivi e degli strumenti informatici che vengono messi a disposizione del personale ai fini dell'esecuzione dell'attività lavorativa nonché di tutte le informazioni, le registrazioni ed i dati inerenti all'esercizio della propria attività che siano contenuti e/o trattati mediante utilizzo di tecnologie informatiche.

Ad ogni dipendente e/o collaboratore può essere assegnato uno o più dispositivi e strumenti informatici (personal computer, laptop, palmare, cellulare, etc.), tramite cui è possibile accedere ad una serie di risorse che possono essere fisicamente ubicate all'interno dei locali della Società o all'esterno della stessa.

L'autorizzazione all'utilizzo dei dispositivi e degli strumenti informatici, quali a titolo esemplificativo e non esaustivo l'accesso alle risorse della rete della Società, alla posta elettronica e ad Internet, concessa al dipendente al momento dell'assunzione o all'inizio del rapporto con il collaboratore, può essere revocata in qualsiasi momento da parte della Società.

L'utilizzo degli strumenti e delle risorse informative della Società deve essere strettamente vincolato all'esercizio delle attività lavorative, rispettando le normative interne e in ottemperanza alle disposizioni legislative vigenti. È proibito l'impiego delle risorse della Società per scopi personali o di terzi.

In particolare, si fa divieto esplicito di:

- Utilizzare le risorse per profitto personale;
- Impiegare le risorse per finalità diverse da quelle per le quali sono state progettate o utilizzare i sistemi informativi per compiere azioni illecite nei confronti di altri sistemi, sia interni che esterni, all'organizzazione;
- Recare volontariamente danni alle risorse della Società, ai sistemi informatici di pubblica utilità, agli strumenti di supporto, ai locali ed in generale ai dispositivi informatici utilizzati dall'organizzazione.

Ogni strumento o risorsa, concessa ai fini esclusivamente lavorativi, deve essere correttamente custodito e mantenuto in buono stato dall'utente che deve contribuire, in rapporto alle proprie responsabilità, alla protezione del patrimonio della Società.

Postazioni di lavoro

La Postazione di Lavoro (di seguito postazione) è costituita dall'insieme di componenti hardware e software forniti all'utente o di proprietà dell'utente ed autorizzate dal rispettivo ente; essa consente l'accesso al complesso dei sistemi e servizi resi disponibili.

L'utente è consapevole e accetta di restituire la totalità delle risorse utilizzate nel momento in cui cessa il rapporto con ciascun ente. Ogni utente, di norma, è assegnatario o autorizzato all'uso di una sola postazione, fissa o mobile; è responsabile della medesima e deve custodirla con diligenza (sia all'interno dell'edificio della Società, sia al di fuori), nonché segnalare eventuali furti, danneggiamenti o smarrimenti.

Inoltre, è tenuto a prestare la massima collaborazione sia alle attività di censimento ed inventario delle risorse hardware e software, sia alle attività di aggiornamento di tali risorse.

Utilizzo del Personal Computer

Il Personal Computer (PC) installato presso la Postazione di Lavoro o fornito all'Utente è configurato in modo ottimale, tenuto conto delle necessità professionali e lavorative.

Il PC affidato al dipendente o collaboratore è uno strumento di lavoro; non ne è pertanto consentita l'utilizzazione non inerente all'attività lavorativa. A tale scopo l'utente potrà utilizzare le risorse disponibili sul proprio PC e dovrà salvare, se necessario, ogni appunto creato sulla memoria di massa del PC stesso (disco locale).

Il PC deve essere custodito con cura evitando ogni possibile forma di uso non autorizzato o di danneggiamento. Il PC dato in affidamento all'utente permette l'accesso alla rete della Società solo attraverso specifiche credenziali di autenticazione, secondo le "regole" definite dalla Società stessa.

Il PC che viene consegnato all'Utente contiene tutti i software necessari a svolgere gli incarichi affidati. Alla cessazione del rapporto intercorso con l'utente, il Personal Computer dovrà essere restituito nella sua interezza, comprese eventuali periferiche interne ed esterne.

Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dalla società, né viene consentito agli utenti di installare autonomamente programmi di qualsivoglia natura, sussistendo infatti il grave pericolo di introdurre Virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone la Società a gravi responsabilità civili; si evidenzia, inoltre, che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore vengono sanzionate anche penalmente.

Salvo preventiva espressa autorizzazione della Società, non è consentito all'Utente modificare le caratteristiche impostate sul proprio PC, né procedere ad installare dispositivi di memorizzazione, comunicazione o altro, come ad esempio masterizzatori, modem, ecc.

In ogni caso, all'utente non è consentito:

- modificare le configurazioni già impostate sul PC consegnato;
- modificare impostazioni di sistema che abbiano un impatto sulla sicurezza o la funzionalità del sistema;
- impedire in qualsiasi modo (personal firewall, cambio di diritti di accesso, rimozione delle condivisioni di sistema, ecc.) l'accesso al software installato sul proprio PC e ai documenti ivi registrati;
- utilizzare programmi e/o sistemi di crittografia senza la preventiva autorizzazione scritta della Società;

- installare alcun software né alcuna versione diversa, anche più recente, rispetto alle applicazioni o al sistema operativo presenti sul PC consegnato, senza l'espressa autorizzazione della Società;
- fare copia del software installato al fine di farne un uso personale;
- fare copia dei documenti in modo diverso dalla copia di back-up prevista dalle procedure interne;
- caricare alcun documento, file musicale o audiovisivo o immagine diversi da quelli necessari allo svolgimento delle mansioni affidate;
- aggiungere o collegare dispositivi hardware (hard disk, drive, PMC, USB, seriale, firewall ecc.) o periferiche (telecamere, macchine fotografiche ecc.) diversi da quelli consegnati, senza l'autorizzazione espressa della Società;
- creare o diffondere programmi idonei a danneggiare il sistema informatico della Società, quali per esempio virus, trojan horses, ecc.;
- impostare connessioni private ad Internet o ad altre reti, ovvero connessioni private di comunicazione verso dispositivi mobili (telefoni cellulari e palmari) (ad es. Bluetooth);
- rimuovere la protezione all'accesso al PC, ovvero lo screensaver a tempo (max 10 minuti);
- utilizzare il PC per scopi privati e comunque non inerenti all'attività lavorativa, salvo quanto specificato riguardo le modalità di utilizzo di Internet e della posta elettronica di seguito riportate.

Al fine di ridurre al minimo i rischi sopra evidenziati, non vengono concessi diritti di Amministratore del sistema operativo e, in caso di necessità, possono essere automaticamente forzate alcune impostazioni di sicurezza (ad esempio lo screensaver con password). I dischi fissi locali del PC sono gestiti sotto la responsabilità dell'utente che deve preoccuparsi di salvare, cancellare e proteggere le informazioni ivi presenti. Al momento della restituzione del PC, tutti i dati presenti sulla memoria di massa locale vengono definitivamente cancellati senza effettuarne alcuna copia.

Ogni utente è tenuto ad operare, con la necessaria diligenza, la custodia dei dati salvati sul proprio PC e non in rete. Considerato che i dati potrebbero accidentalmente essere perduti o danneggiati, l'utente deve valutare se conservare copia dei files presenti registrati sul disco fisso del proprio PC. Se l'eventuale copia fosse effettuata su supporti informatici (dispositivi USB, CD-ROM, DVD, Memory Card, Cellulari ecc.) gli stessi dovranno essere custoditi in modo adeguato al tipo di informazioni contenute e dovranno essere distrutti o cancellati quando le suddette informazioni non saranno più utili.

Nell'utilizzo della postazione di lavoro è opportuno non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

È opportuno terminare la sessione di lavoro svolta tramite utilizzo di un personal computer, ogni volta che ci si deve allontanare, anche solo per un breve periodo, effettuando il "log out" dell'account utente o mettendo in atto accorgimenti tali per cui il PC non resti:

- incustodito: può essere sufficiente, a titolo esemplificativo, che un collega rimanga nella stanza durante l'assenza di chi sta utilizzando il PC anche se la stanza rimane aperta;
- accessibile: può essere sufficiente chiudere a chiave la stanza all'interno della quale è situato lo strumento elettronico.

Non devono mai verificarsi situazioni in cui un Personal Computer venga lasciato attivo, durante una sessione di trattamento, senza che sia controllato da un Autorizzato al trattamento o senza che la stanza in cui è ubicato venga chiusa a chiave.

È possibile predisporre strumenti software specifici (es.: screen saver) che, trascorso un breve periodo di tempo predeterminato in cui l'elaboratore resta inutilizzato, non consente più l'accesso all'elaboratore se non previo inserimento di credenziali di accesso (es.: password, ecc.).

L'utente è tenuto a dare tempestiva segnalazione ai referenti IT di eventuali anomalie o irregolarità nel funzionamento del PC consegnato, al fine di prevenire la perdita totale o parziale della riservatezza, integrità e/o disponibilità delle informazioni in esso contenute nonché di prevenire eventuali guasti all'intero sistema. All'utente non è consentito stampare un documento elettronico, contenente informazioni riservate, trasformandolo in un documento cartaceo, se non solo ed esclusivamente per esigenze di lavoro. In tale ipotesi, il grado di riservatezza e segretezza delle informazioni contenute nel documento cartaceo dovrà ritenersi esattamente equivalente a quello delle medesime informazioni contenute nel documento elettronico trasformato mediante stampa. L'utente dovrà assicurare alle informazioni riservate contenute nel documento cartaceo una protezione adeguata ed equivalente a quella richiesta per i documenti elettronici corrispondenti.

Per ogni necessità interna, il personale espressamente incaricato ed autorizzato dalla società quale Amministratore di Sistema potrà accedere alla memoria di massa locale del PC e ai server nonché, previa comunicazione all'utente, accedere al PC di quest'ultimo anche in modalità "da remoto".

Al personale espressamente incaricato dalla società quale Amministratore di Sistema è riconosciuta la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

Inoltre, dal momento che la violazione delle regole di cui sopra potrebbe esporre la società al rischio di danneggiamento del sistema informatico, il loro rispetto potrebbe essere oggetto di controllo attraverso periodiche verifiche del contenuto della memoria di massa dei server oltre che del PC consegnato.

Utilizzo di dispositivi rimovibili

La postazione e gli eventuali supporti di memoria rimovibili (CD, chiavi USB, memory card ecc.) devono essere conservati in luoghi protetti; è sempre necessario verificare il contenuto informativo dei supporti di memoria, prima della loro consegna a terzi e prima della loro eliminazione / distruzione. L'utente non è autorizzato ad accedere, né a tentare l'accesso alle informazioni per le quali non ha alcun privilegio; è altresì vietato tentare di guadagnare privilegi non concessi dal proprietario del dato.

Tutti i supporti magnetici rimovibili (CD, DVD riscrivibili, supporti USB, memory card, cellulari ecc.), contenenti dati "sensibili" nonché informazioni costituenti patrimonio della Società, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato. Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati "sensibili", ogni utente dovrà contattare il personale IT della Società e seguire le istruzioni da questo impartite. In ogni caso, i supporti magnetici contenenti dati sensibili devono essere adeguatamente custoditi dagli utenti in armadi chiusi. L'utente è responsabile della custodia dei supporti e dei dati in essi contenuti.

Credenziali di autenticazione

Le credenziali di autenticazione ai sistemi informatici, generalmente composte da un “identificativo utente” (c.d. username o user) al quale è associata una specifica “password”, sono informazioni di carattere assolutamente personale e non cedibili, per nessuna ragione.

Se si è in possesso di più credenziali di autenticazione, è necessario fare attenzione ad accedere ai dati unicamente con le credenziali relative al trattamento in oggetto. Nell'utilizzo delle credenziali di autenticazione l'utente è tenuto a rispettare:

- l'ambito di competenza assegnato;
- le base dati a cui poter accedere;
- il profilo di autorizzazione assegnato;
- le tipologie di trattamento consentito;

segnalando tempestivamente eventuali anomalie e/o malfunzionamenti riscontrati.

Scelta della password

Elaborare le password seguendo le istruzioni sotto riportate.

Il più semplice metodo per l'accesso illecito a un sistema consiste nell'indovinare la password dell'utente legittimo. In molti casi sono stati procurati seri danni al sistema informativo a causa di un accesso protetto da password "deboli". La scelta di password "forti" è, quindi, parte essenziale della sicurezza informatica.

Di norma la password deve essere composta da **almeno otto caratteri** o, se il sistema non l'accetta, da un numero di caratteri pari a quello consentito dal sistema; è buona norma che, di questi caratteri, da un quarto alla metà siano di natura numerica.

L'utente deve provvedere a modificare la password immediatamente, non appena la riceve per la prima volta, da chi amministra il sistema.

La password deve essere modificata dall'utente con una frequenza di **almeno 6 mesi** o nel caso in cui il sistema lo preveda, alle scadenze proposte dal sistema stesso.

Se il trattamento riguarda categorie particolari di dati o dati di natura giudiziaria, la password deve essere modificata con frequenza maggiore (es.: **ogni 3 mesi**).

Di seguito sono riportate alcune indicazioni “utili” per la scelta di una password

Cose da fare

- ✓ Creare password lunghe e/o utilizzare più di una parola (a volte è più semplice ricordare una frase completa di senso compiuto piuttosto che una parola complicata, e questa tecnica oltre a facilitare la memorizzazione migliora la sicurezza stessa della parola chiave: la lunghezza influisce sulle difficoltà di individuazione e ci consente di utilizzare lo "spazio" tra una parola e l'altra come ulteriore elemento da intercettare);

- ✓ È utile sapere che la maggior parte degli “strumenti di intercettazione” presumono che le password non siano formate da più di 14 caratteri, e quindi, anche senza complessità, le password molto lunghe (da 14 a 128 caratteri) possono rappresentare un’ottima protezione contro possibili violazioni (non tutti i software sono tuttavia in grado di accettare password superiori a 14 caratteri);
- ✓ Utilizzare numeri e simboli al posto di caratteri;
- ✓ Non limitarsi alle sole lettere ma, dove possibile, utilizzare l'ampia gamma di minuscole/maiuscole, numeri e simboli a disposizione sulla propria tastiera:
 - Caratteri minuscoli: Es.: a, b, c,
 - Caratteri maiuscoli: Es.: A, B, C,
 - Caratteri numerici: Es.: 0,1,2,3,4,5,6,7,8,9
 - Caratteri non alfanumerici: Es.: < > ` ~ ! \$ % ^ ; * - + = | \ { @ # } [/] : ; " ' ?
- ✓ Non inserire i “caratteri speciali” alla fine di una parola nota (ad esempio la password “computer987” può essere identificata abbastanza facilmente - la parola “computer” è inclusa in molti dizionari contenenti nomi comuni e quindi dopo aver scoperto il nome restano solo 3 caratteri da identificare);
- ✓ Sostituire una o più lettere all'interno della parola con simboli che possono essere ricordati facilmente (ad esempio si può provare a utilizzare “@” al posto di “A”, “\$” al posto di “S”, zero (0) o la doppia parentesi () al posto di “O”, e “3” al posto di “E”). Si tratta di trovare delle analogie che ci rendano familiare la sostituzione di lettere con simboli e numeri (con alcune sostituzioni si possono creare password riconoscibili per l'utente, ad esempio “Ve\$tit0 di Mari0”, già sufficientemente lunghe e estremamente difficili da identificare o decifrare).
- ✓ Cercare di realizzare password utilizzando caratteri appartenenti a tutti i quattro gruppi rappresentati nella lista sopra riportata.

Cose da NON fare

- ❖ NON divulgare la propria password: lo scopo principale per cui si usa una password è assicurare che nessun altro possa utilizzare le risorse o possa farlo per conto dell’utente;
- ❖ NON scrivere la password in nessun posto in cui possa essere letta facilmente, soprattutto vicino al PC;
- ❖ In fase di immissione della password assicurarsi di non essere osservato;
- ❖ NON scegliere password che siano contenute all’interno di un dizionario: su alcuni sistemi è possibile “provare” tutte le password contenute in un dizionario per individuare quale giusta (l’utilizzo di parole straniere non consente di aggirare tale problema);
- ❖ NON è opportuno utilizzare il “nome utente” quale password (è la password più semplice da indovinare);
- ❖ NON è opportuno utilizzare password che possano in qualche modo essere facilmente collegate all’utente (Es.: nome, nome della moglie / marito, nome dei figli, del cane, date di nascita, numeri di telefono, ecc.).

Antivirus

Ogni utente deve accertarsi che, sulla propria postazione di lavoro, il software antivirus sia sempre aggiornato e funzionante, secondo quanto definito dalla società.

Non è consentito agli utenti disabilitare o inibire il corretto funzionamento del software antivirus eventualmente installato sulla propria Postazione di Lavoro, o modificarne la configurazione, disabilitando o disattivando i meccanismi di notifica automatica degli eventi e di segnalazione degli allarmi.

Qualora per la propria postazione di lavoro non esista un software antivirus rispondente alle norme, o non sia possibile installare correttamente il software antivirus, l'utente dovrà informare immediatamente il proprio Responsabile.

Nel caso in cui il software antivirus rilevi la presenza di un virus che non è riuscito ad eliminare, l'utente deve immediatamente sospendere ogni elaborazione in corso, senza spegnere il computer e segnalare l'accaduto ai referenti IT della Società.

Non è consentito agli utenti rimuovere virus con azioni personali, ma è necessario avvalersi dell'assistenza necessaria, attenendosi alle modalità stabilite dalle eventuali procedure di "gestione degli incidenti"; ad operazione ultimata, gli utenti devono accertarsi dell'eliminazione del virus e della riusabilità della Postazione di Lavoro.

Sistemi di backup

Per ogni applicazione utilizzata dalla Società devono essere previste attività di backup periodico per le quali sono definiti i seguenti aspetti:

- la frequenza di esecuzione dell'attività;
- le modalità di effettuazione;
- il numero di copie da produrre;
- il periodo di conservazione dei dati.

I servizi di backup devono essere adeguati in relazione alla tipologia di dati contenuti all'interno delle diverse applicazioni e devono essere volti a garantire che tutte le informazioni essenziali e il software possano essere recuperati a seguito di un guasto o di un disastro.

Durante la progettazione di un sistema di backup, devono essere presi in considerazione i seguenti elementi:

- misura (ad esempio, completo o differenziale di backup) e frequenza dei backup devono riflettere le esigenze di business dell'organizzazione, i requisiti di sicurezza delle informazioni in questione e la criticità delle informazioni per il continuo funzionamento dell'organizzazione;
- i backup devono essere memorizzati in una posizione remota (con protezione ambientale e fisica), ad una distanza sufficiente per sfuggire ai danni eventualmente provocati da un disastro al luogo principale;
- supporti di backup devono essere testati regolarmente per garantire che possano essere effettivamente utilizzati in caso di emergenza.

È opportuno prevedere specifiche procedure interne per monitorare l'esecuzione dei backup e degli eventuali fallimenti, al fine di garantire la completezza dei backup stessi. Nel caso di sistemi e servizi critici, le modalità di backup devono coprire tutti i sistemi informativi, applicazioni e dati necessari per ripristinare il sistema completo in caso di disastro. Il periodo di conservazione deve essere determinato, tenendo conto di ogni esigenza dell'organizzazione.

OPERATIVITÀ SU BANCHE DATI

È raccomandabile, laddove possibile, che l'estrazione, la copia, il salvataggio e la stampa su qualunque supporto d'informazioni contenute in banche dati sia precluso, mediante adozione di idonei dispositivi tecnologici e strumenti organizzativi, a tutti gli utenti con la sola esclusione di quelli a ciò specificamente autorizzati per ragioni tecniche. Tale previsione non risulta applicabile alle banche dati funzionali al raggiungimento delle finalità istituzionali della Società e utilizzate per lo svolgimento dei propri servizi, ovvero che siano prodotte e commercializzate con espressa concessione di tali facoltà in virtù della loro natura di strumenti di diffusione di determinati contenuti informativi.

SERVIZI DI RETE

Nell'utilizzo della rete interna gli utenti devono tenere un comportamento corretto e diligente. A tal riguardo, l'utente non deve effettuare nessun tipo di attività volta ad eludere o compromettere i meccanismi di protezione dei sistemi informatici.

Per l'accesso alla rete della Società ciascun utente deve essere in possesso della specifica credenziale di autenticazione. È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. La parola chiave d'ingresso alla rete ed ai programmi è segreta e deve essere comunicata e gestita con la massima riservatezza nel rispetto delle eventuali procedure interne definite.

Le cartelle utenti presenti nei server della Società sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità, sulle quali vengono, peraltro, svolte regolari attività di controllo, amministrazione e back up da parte del personale IT della Società.

Conseguentemente, agli utenti non è consentito conservare, salva espressa autorizzazione della Società:

- dati non relativi all'attività della Società;
- copie di software ed applicativi;
- files o filmati (.MPEG, .AVI, .MOV, ecc.) o musica (.WAV, .MP3, ecc.).

Ciascun ente può, in qualunque momento, previo avviso al dipendente o collaboratore (fatti salvi i casi di urgenza e gravità), procedere alla rimozione di ogni file o applicazione che riterrà pericolosi per la sicurezza del sistema, sia dai PC degli incaricati sia dalle unità di rete.

È opportuno che, con regolare periodicità, ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

L'accesso alla rete è consentito solo ai PC che siano usati conformemente alle regole definite da ciascun ente. Il dipendente o il collaboratore è tenuto a dare tempestiva segnalazione di eventuali anomalie o irregolarità nel funzionamento delle risorse di rete, al fine di prevenire la perdita totale o parziale della riservatezza, integrità e/o disponibilità delle informazioni in esse contenute nonché di prevenire eventuali guasti all'intero sistema.

Per motivi di urgenza, ovvero per provvedere alla manutenzione dei sistemi informativi, il personale espressamente incaricato dalla società può accedere ai server ed alle aree di condivisione di informazioni. In particolare, il personale incaricato dalla società, nella qualità di Amministratore di Sistema, è autorizzato a compiere interventi nel sistema informativo diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/ sostituzione/ implementazione di programmi, manutenzione hardware etc.). Detti interventi, potranno anche comportare l'accesso, in qualunque momento, ai dati trattati da ciascun utente.

Inoltre, dal momento che la violazione delle regole di cui sopra potrebbe esporre la società al rischio di danneggiamento o mal funzionamento del sistema informatico, il rispetto di tali regole potrebbe essere oggetto di controllo attraverso periodiche verifiche del contenuto della memoria di massa dei server oltre che del PC consegnato all'utente. Tale controllo costituisce una procedura di controllo di carattere "ordinario" (o di 1° livello), rivolta principalmente in modo indistinto alla popolazione della Società, giustificata da esigenze operative, organizzative e produttive della Società nonché dalla necessità di tutela del patrimonio informativo della Società stessa, e potrà essere eseguita anche mediante l'utilizzo di strumenti automatizzati. L'accesso ai sistemi ed alle evidenze del controllo è riservato esclusivamente al personale incaricato dalla società quale Amministratore di Sistema.

UTILIZZO DI INTERNET

Il servizio di connessione ad Internet della Società è uno strumento operativo che viene reso disponibile agli utenti che ne abbiano effettiva necessità.

L'accesso ad Internet è fornito allo scopo di ottenere informazioni necessarie allo svolgimento dell'attività lavorativa. Essendo uno strumento di lavoro di proprietà di CARBOSULCIS SPA, i soggetti cui la società attribuisce l'accesso sono responsabili del suo corretto utilizzo.

Esso costituisce una risorsa ed un'opportunità di sviluppo della Società, ma rappresenta anche una potenziale minaccia alla sicurezza dei sistemi e delle informazioni. L'uso incauto può essere una fonte di rischio per la sicurezza, oltre che un costo rilevante per gli enti.

La Società, qualora lo ritenga necessario, ha la facoltà di revocare l'accesso ad Internet dei singoli utenti e di installare software atti a filtrare / bloccare in automatico l'accesso a siti che non sono ritenuti di interesse della Società o attinenti ad attività lavorative. L'utente che accede ad un sito Internet deve prendere visione se specificato nel sito stesso, dei termini e le condizioni che ne regolano l'utilizzo e operare in conformità delle stesse.

L'uso di Internet attraverso le apparecchiature della Società è consentito solo per motivi di lavoro e nell'interesse esclusivo della Società. La connessione ad Internet dai computer (inclusi portatili e palmari) e ogni accesso alla rete Internet potrebbero essere registrati nel proxy Server della Società.

L'accesso ad Internet deve avvenire solo attraverso le infrastrutture tecnologiche poste in essere dalla società e deve essere configurato dal personale IT specializzato. Non è autorizzato pertanto l'accesso a Internet utilizzando collegamenti via modem o altri mezzi di collegamento personali.

L'utente si impegna, nei confronti della Società cui appartiene, a non utilizzare il servizio di connessione ad Internet per scopi illegali o che comunque possano recare danno o pregiudizio alla medesima o a terzi, assumendosi ogni responsabilità derivante dall'uso improprio del servizio ed esonerando contestualmente la società da ogni pretesa o azione che dovesse essere rivolta alla medesima da qualunque soggetto, in conseguenza di tale uso improprio.

L'utente, inoltre, non può utilizzare la connessione a Internet in modo da danneggiare, disattivare, sovraccaricare, pregiudicare o interferire con l'utilizzo e il godimento della stessa da parte di altri Utenti. In ogni caso al dipendente o collaboratore non è consentito:

- accedere ai siti Internet assoggettati a restrizione da parte della Società, forzando i sistemi di sicurezza dalla medesima predisposti ed in ogni caso utilizzare siti o altri strumenti (es. Cracking Programs) che realizzino tale fine;
- effettuare il download di software, ancorché gratuito (freeware), o messo a disposizione in rete per essere provato (shareware, demo), e comunque il download di qualsiasi software nonché di file multimediali (come file musicali o video) senza l'espressa autorizzazione della Società;
- modificare la configurazione del browser o del PC in modo da diminuirne il livello di protezione Internet;
- effettuare qualsiasi genere di attività personale di guadagno economico, nonché di transazione finanziaria in rete, ivi compresi gli acquisti on line e le operazioni di remote banking per scopi estranei allo svolgimento dell'attività lavorativa;

- accedere a siti Internet che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico;
- utilizzare Internet per effettuare attività considerate illegali e, comunque, accedere a siti contenenti:
 - materiale teso alla promozione di comportamenti criminali o violenti;
 - materiale discriminante o lesivo in relazione a razza, sesso, religione, ecc.;
 - materiale che violi la legge in materia di protezione dati personali;
 - contenuti o materiali che violino i diritti di proprietà di terzi;
 - materiale pornografico o simile, in particolare in violazione della legge n.269 del 1998 "Norme contro lo sfruttamento sessuale dei minori degli anni 18";
 - altri contenuti inappropriati o contrari alla legge;
- accedere, attraverso le apparecchiature della Società, a qualsivoglia gruppo di discussione o conferenza in rete (chat lines o altro) o banche dati esterne, con la sola esclusione di quelli espressamente autorizzati;
- utilizzare identificativi altrui al fine di effettuare la connessione a Internet;
- utilizzare l'accesso ad Internet in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore.

Qualunque attività eseguita in Internet deve tenere conto, in qualunque momento, dell'integrità dei dati della Società, per esempio: non si devono divulgare informazioni tecniche quali IP address, password o identificativi utenti.

La Società potrebbe utilizzare prodotti di *Content Filtering* per selezionare il traffico di Internet e si potrebbe dotare di apposite procedure per la gestione dei profili di accesso al servizio, che regolamentano e limitano l'accesso al servizio e ad alcuni siti.

Il dipendente è tenuto a dare tempestiva segnalazione di eventuali anomalie o irregolarità nel funzionamento dell'accesso a Internet, al fine di prevenire eventuali guasti all'intero sistema.

Dal momento che la violazione delle regole sopra riportate potrebbe esporre la società al rischio di danneggiamento o mal funzionamento del sistema informatico, il rispetto di tali regole potrà essere oggetto di controllo anche mediante accesso in remoto, attraverso periodiche verifiche del contenuto della memoria di massa dei server di accesso a Internet (proxy), dei PC e dei sistemi di "Content Filtering", nonché mediante esame dei file di log della navigazione svolta.

Tale controllo costituisce una procedura di controllo di carattere "ordinario" (o di 1° livello), rivolta principalmente in modo indistinto alla popolazione della Società, giustificata da esigenze operative, organizzative e produttive della Società nonché dalla necessità di tutela del patrimonio informativo della Società stessa, e potrà essere eseguita anche mediante l'utilizzo di strumenti automatizzati. L'accesso ai sistemi ed alle evidenze del controllo è riservato esclusivamente al personale della Società individuato quale "Amministratore di Sistema".

POSTA ELETTRONICA

La Società può attribuire agli utenti un "Account" o indirizzo di posta elettronica utilizzabile per inviare e ricevere e-mail. La casella di posta elettronica assegnata all'utilizzatore, il relativo indirizzo e i messaggi in entrata ed in uscita dalla stessa, sono di proprietà della Società. Essi rappresentano uno strumento di lavoro affidato all'utente al solo fine di consentirgli di svolgere le proprie mansioni ed attività lavorativa.

Le persone cui la società attribuisce l'uso di caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti. Il personale incaricato dalla società quale Amministratore di Sistema, inoltre, è autorizzato a compiere interventi nel sistema informativo della Società diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento / sostituzione / implementazione di programmi, manutenzione hardware etc.). Tali interventi, potranno anche comportare l'accesso in qualunque momento alle caselle di posta elettronica degli utenti, escludendo tuttavia che l'accesso sia finalizzato, in tali circostanze, ad attività di controllo.

Utilizzando l'indirizzo di posta elettronica della Società, l'utente è a conoscenza e consapevole che:

- un messaggio di posta elettronica si configura, da un punto di vista giuridico, come corrispondenza aperta, potendo essere letto da chiunque durante il suo percorso sulla rete Internet fino al destinatario, nonché dall'Amministratore di sistema sui server;
- l'uso dell'indirizzo di posta elettronica della Società è ammesso per motivi attinenti all'attività lavorativa: l'uso per motivi personali è consentito solo nei limiti della normalità e cioè per un limitato numero di messaggi di cortesia o inerenti rapporti parentali o amicali, sempre nel rispetto delle norme di comportamento interne e tenuto conto dell'interesse della Società;
- a tutela del proprio diritto alla privacy, relativa ai messaggi di posta elettronica in entrata ed in uscita utilizzando l'indirizzo della Società, l'accesso ai messaggi personali ivi contenuti, qualora esso si dovesse rendere necessario (es. in caso di assenza non programmata dell'utente), oppure per motivazioni di carattere lavorativo ed a giudizio della Società, può avvenire per il tramite di altro collega (fiduciario) indicato dal dipendente stesso. Sarà comunque consentito al superiore gerarchico o, sentito l'utente (qualora raggiungibile), a persona individuata dalla società, accedere alla propria casella di posta elettronica per ogni ipotesi di carattere lavorativo per cui ciò si dovesse rendere necessario. Il fiduciario, che agirà all'occorrenza in caso di assenza dell'utente, ovvero il superiore gerarchico, o la persona individuata dalla società come sopra indicato, utilizzerà una password d'ingresso creata "ad hoc" dal fiduciario (ovvero dal superiore gerarchico o persona individuata dalla società) mediante autorizzazione della Società. La password dovrà essere custodita dal fiduciario (ovvero dal superiore gerarchico o persona individuata dalla società) e dovrà essere resettata al cessare delle suddette motivazioni o al rientro del titolare. È cura dell'utente segnalare al proprio superiore gerarchico il nominativo del fiduciario prescelto;
- il messaggio di posta elettronica potrebbe essere letto da destinatari diversi da quelli a cui era diretto, e ciò potrebbe determinare danni anche gravi alla società;
- falsi o errati messaggi di posta elettronica scritti per conto e nel nome della Società potrebbero essere spediti

- per errore sia all'interno che all'esterno della Società;
- messaggi di posta elettronica spediti potrebbero non essere recapitati, essere distrutti o subire ritardi. In ogni caso al dipendente o collaboratore non è consentito:
- inviare un messaggio con allegato un file eseguibile (.exe);
- utilizzare l'indirizzo di posta elettronica contenente il dominio della Società per iscriversi a qualsivoglia sito per motivi non attinenti all'attività lavorativa, senza espressa autorizzazione scritta della Società, nonché per partecipare a qualunque genere di petizione, "catene di Sant'Antonio" o in generale, a qualunque pubblico dibattito su qualsivoglia tema;
- indicare liberatorie personalizzate all'interno dei messaggi;
- utilizzare il servizio di posta elettronica per trasmettere a soggetti esterni alla Società informazioni riservate o documenti interni, se non nel caso in cui ciò sia necessario in base alle mansioni svolte;
- accedere a caselle di posta elettronica personali attraverso la rete (Webmail) e le apparecchiature della Società. L'utente non potrà, peraltro, inoltrare automaticamente i messaggi ricevuti all'indirizzo di posta elettronica della Società su indirizzi personali;
- inviare o archiviare messaggi in forma crittografata senza l'espressa autorizzazione che deve essere richiesta ai referenti IT;
- inviare, tramite la posta elettronica, anche all'interno della rete della Società, alcun materiale a contenuto violento, sessuale o comunque offensivo dei principi di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazione del pensiero, anche politico. Qualora il dipendente riceva messaggi aventi tale contenuto, è tenuto a darne comunicazione tempestiva al proprio responsabile;
- ricevere ed inviare messaggi con allegati diversi da quelli inerenti alla prestazione lavorativa;
- creare, archiviare o spedire, anche all'interno della rete della Società, messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) in nessun modo connessi con lo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto utilizzando l'indirizzo della Società;
- utilizzare la posta elettronica della Società in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore.

Il dipendente o il collaboratore è tenuto a dare tempestiva segnalazione di eventuali anomalie o irregolarità nel funzionamento della posta elettronica, al fine di prevenire la perdita totale o parziale della riservatezza, integrità e/o disponibilità delle informazioni in essa contenute nonché di prevenire eventuali guasti all'intero sistema.

Dal momento che la violazione delle regole sopra riportate potrebbe esporre la società al rischio di danneggiamento o mal funzionamento del sistema informatico, il rispetto di tali regole potrebbe essere oggetto di controllo attraverso periodiche verifiche del contenuto della memoria di massa dei server oltre che del PC consegnato al dipendente. Tale controllo costituisce una procedura di controllo di carattere "ordinario" (o di 1° livello), rivolta

principalmente in modo indistinto alla popolazione della Società, giustificata da esigenze operative, organizzative e produttive della Società nonché dalla necessità di tutela del patrimonio informativo della Società stessa, e potrà essere eseguita anche mediante l'utilizzo di strumenti automatizzati. L'accesso ai sistemi ed alle evidenze del controllo è riservato esclusivamente al personale della Società individuato quale "Amministratore di Sistema".

COLLEGAMENTO REMOTO

Il collegamento remoto a reti, sistemi o applicazioni della Società è consentito esclusivamente per finalità interne attraverso i punti di ingresso identificati ed autorizzati (server di posta, concentratori VPN, o altro) e per il tempo strettamente necessario all'esecuzione delle attività lavorative.

Il collegamento tramite computer non della Società è consentito esclusivamente se preventivamente autorizzato o per gravi e motivate situazioni di emergenza. In ogni caso, il computer utilizzato deve essere dotato di sistemi antivirus, attivi ed aggiornati. È vietato il collegamento da dispositivi pubblici, ad esempio Internet point.

**SISTEMI DI TELEFONIA*

L'utilizzo delle credenziali di accesso ai sistemi di telefonia che lo prevedono (VoIP o cellulari di lavoro) costituisce a tutti gli effetti un accesso a rete o sistema, con l'assunzione di responsabilità da parte dell'utente che ne consegue per le operazioni successivamente eseguite. I telefoni cellulari di lavoro devono essere impostati con la richiesta del PIN all'accensione. Ove possibile deve essere attivata la funzione di crittografia automatica del dispositivo portatile in caso di spegnimento dell'apparato.

ACCESSO AI SISTEMI

L'accesso ai sistemi, alle reti ed alle applicazioni deve essere preventivamente autorizzato e deve svolgersi con modalità conformi allo svolgimento delle attività della Società. La società attribuisce ad ogni utente delle credenziali di autenticazione (user-id e password) per l'accesso alle risorse e alla rete locale. L'accesso deve avvenire esclusivamente attraverso l'utilizzo della utenza personale (user-id) assegnata o, in casi particolari per finalità di test, assistenza o manutenzione, con altra, apposita utenza.

La mera possibilità di utilizzo di sistemi, reti o applicazioni per le quali non si sia stati preventivamente autorizzati non costituisce una implicita autorizzazione, ma al contrario è da ritenere una possibile esposizione di sicurezza da segnalare alle strutture competenti. L'accesso ai sistemi, alle reti ed alle applicazioni è sottoposto a registrazione. Le credenziali di accesso, costituendo la base per l'identificazione e l'autenticazione degli utenti nella fase di accesso ai sistemi informatici, devono essere custodite con la massima riservatezza e non rivelate ad alcuno (neanche ai colleghi). Qualunque accesso effettuato utilizzando le credenziali personali dell'utente è da considerare sotto la diretta responsabilità dell'utente stesso così come lo sono le conseguenti operazioni effettuate.

Analogha riservatezza deve essere osservata nei confronti delle credenziali di accesso "applicative" (cioè delle credenziali utilizzate da applicazioni, sistemi o dispositivi) di cui si venga a conoscenza. Qualora l'utente ritenga che la confidenzialità delle credenziali sia stata compromessa, deve provvedere, nel caso di password, al cambio immediato della stessa, o, nel caso di credenziali di autenticazione di altro genere (smart card, token, ecc.), all'immediata segnalazione ai referenti IT. Le credenziali di accesso rilasciate all'utente sono conservate con modalità che non ne consentono la conoscenza o la ricostruzione, neanche da parte del personale IT.

PROTEZIONE DEI DATI – TECNICHE DI SOTTRAZIONE

Informazioni di normale utilizzo nel corso dell'attività operativa della società o ritenute non riservate nell'ambito delle comunicazioni interne tra il personale aziendale, potrebbero assumere una diversa importanza se comunicate all'esterno a soggetti terzi, necessitando quindi di una maggiore tutela.

La salvaguardia delle informazioni e dei dati oltre ad essere un requisito fondamentale per la sicurezza del patrimonio informativo aziendale, è anche un espresso obbligo di legge nei confronti di qualsiasi soggetto definito "interessato". A fronte di tali motivazioni è importante sottolineare la necessità di osservare ogni cautela nel trasferire all'esterno qualsiasi informazione proporzionalmente al loro contenuto e all'attendibilità dell'interlocutore.

Nel corso anni si sono sviluppate numerose tecniche per la sottrazione “fraudolenta” di dati e informazioni gestiti da parte degli utenti nell'ambito dell'attività lavorativa tra cui le più rilevanti sono:

- il social engineering;
- l'E-mail phishing.

Il social engineering

Il Social Engineering è un insieme di “tecniche psicologiche” usate da chi vuole indurre qualcun altro ai propri scopi presentandosi personalmente presso l'utente o contattandolo dall'esterno a mezzo telefono o posta elettronica. Gli obiettivi possono andare dalla raccolta di informazioni apparentemente innocue riguardanti l'azienda o la sua organizzazione e il personale in forza, ma possono arrivare a raggiungere dati anche molto riservati.

Con l'ausilio di messaggi studiati e abili tecniche di persuasione, l'aggressore può anche rendere l'utente complice inconsapevole di azioni che andranno a suo beneficio come, ad esempio, l'acquisizione di informazioni o l'ottenimento della fiducia degli utenti, l'apertura di allegati infetti o la visita di siti che contiene “dialer” o altro materiale pericoloso.

Uno dei principali problemi degli autori di virus è che molti utenti utilizzano strumenti di difesa aggiornati che non consentono l'esecuzione in automatico di applicativi e quindi non consentono l'attivazione di programmi dannosi. Per scavalcare queste precauzioni e quindi attivare l'azione di un virus, attraverso tecniche di social engineering si potrebbe indurre la vittima, tramite espedienti psicologici, a fidarsi dell'allegato e quindi eseguirlo, o fidarsi del collegamento ad un sito web contenuto nel messaggio e quindi raggiungerlo. In questo modo l'aggressore potrebbe essere capace di sfruttare i punti di debolezza redigendo abili messaggi che, inducendo fiducia o curiosità, riescono ad arrivare allo scopo.

L'E-mail phishing

Altro scopo di possibili aggressori è indurre l'utente a fidarsi dell'intero contenuto di un messaggio di posta elettronica e quindi ottenere una fedele esecuzione delle istruzioni contenute: ad esempio, vengono inviate false comunicazioni e-mail aventi grafica, forma, autorevolezza e loghi ufficiali di enti noti, banche, intermediari finanziari, assicurazioni, etc., chiedendo informazioni attraverso moduli o link a pagine web debitamente camuffate.

Attraverso questa modalità vengono richieste all'utente informazioni riservate (es.: password, numeri di carta di credito, ecc.) senza che in realtà la raccolta dati abbia nulla a che vedere con l'organismo ufficiale imitato. La vittima crede di comunicare con essi ma in realtà sta trasmettendo informazioni riservate all'aggressore.

Le tecniche di sottrazione dati di cui sopra spesso sono abbinate tra loro e applicate più volte nel tempo sulla stessa vittima in modo da poter ottenere dei risultati.

Al fine di ridurre i rischi di sottrazione dati è opportuno:

- evitare di fornire informazioni confidenziali al telefono o di persona a interlocutori non conosciuti;
- limitarsi a fornire informazioni a interlocutori noti e operanti con l'utente per disposizione aziendale nei limiti dei contenuti afferenti all'ambito lavorativo assegnato;
- diffidare di messaggi provenienti da fonte non conosciuta;
- non aprire messaggi provenienti da fonte non conosciuta contenenti allegati;
- non aprire messaggi contenenti allegati sospetti;
- non utilizzare mai link contenuti nel testo del messaggio perché possono essere facilmente falsificati;
- non trasmettere mai alcuna informazione in risposta ad una richiesta proveniente da fonte sconosciuta;
- non trasmettere mai alcuna informazione in risposta ad una richiesta proveniente da fonti istituzionali o apparentemente conosciute (ad es.: banche) in quanto tali strutture non richiedono mai dati utilizzando questa modalità;
- in caso di dubbio è sempre preferibile verificare l'attendibilità delle richieste con il proprio Responsabile.

POLITICHE GENERALI PER L'UTILIZZO DEGLI ARCHIVI CARTACEI

Tutto il materiale cartaceo contenente dati personali deve essere gestito evitando che esso risulti facilmente visibile a persone terze o, comunque, ai non autorizzati al trattamento. Non deve essere lasciato incustodito sulle scrivanie e, a fine lavoro, deve essere riposto in un luogo sicuro.

In caso di trattamento di dati particolarmente c.d. sensibili (condizioni di salute, dati giudiziari, ecc.), tutta la documentazione cartacea deve essere conservata in armadi/cassetti chiusi a chiave o stanze chiuse a chiave in caso di allontanamento, anche temporaneo, dalla postazione di lavoro.

I documenti contenenti dati "sensibili" particolari devono essere controllati e custoditi in modo che non vi accedano persone non autorizzate. La consultazione deve avvenire per il tempo strettamente necessario alla digitazione stessa e, subito dopo, i documenti devono essere archiviati.

Ogni dipendente o collaboratore ha la responsabilità dei propri documenti e in presenza di dati personali, deve:

- consentire l'accesso unicamente per finalità lavorative, a persone autorizzate e limitatamente ai dati la cui conoscenza è strettamente necessaria;
- proteggere i documenti cartacei e i dati personali in essi contenuti da perdite, distruzione, falsificazione, accesso e divulgazione non autorizzati;
- conservare gli atti e i documenti contenenti dati personali in archivi ad accesso selezionato, secondo le istruzioni del proprio responsabile;
- distruggere fisicamente i documenti cartacei che contengono dati personali prima di cestinarli;
- restituire i documenti al termine delle operazioni affidate.