Centro Servizi per le Imprese
Camera di Commercio Cagliari

Azienda Speciale della Camera di commercio di Cagliari-Oristano

Centro Servizi Promozionali per le Imprese

Modello Organizzativo Privacy (MOP)

Ruoli e sistema di responsabilità, ai sensi del Regolamento UE 2016/679, art. 24

Approvato con deliberazione del Consiglio di Amministrazione n. 10 del 06/08/2021

SOMMARIO

ACRONIMI E DEFINIZIONI UTILIZZATE

GDPR	Regolamento UE 2016/679 (General Data Protection Regulation)
Codice	D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali"
Garante	Garante per la protezione dei dati personali
EDPB e WP29	Comitato europeo perla protezione dei dati (European Data Protection Board) che ha sostituito il Gruppo di lavoro ex art. 29 (Working Party article 29)
RPD/DPO	Responsabile della Protezione dei Dati
CDA	Consiglio di Amministrazione dell'Azienda - Titolare
Delegato del Titolare	Soggetto che, secondo le deleghe/procure formalizzate e il sistema di gestione della privacy, garantisce specifiche funzioni ai fini della conformità al GDPR
Referente Privacy	Soggetto che supporta il RPD/DPO
Direttore	Direttore dell'Azienda speciale

PREMESSA

SCOPO E CAMPO DI APPLICAZIONE

Scopo del presente documento è definire il modello organizzativo per la gestione degli adempimenti in materia di protezione dei dati e degli interessati, avendo come riferimento il Regolamento UE 2016/679 sulla protezione dei dati personali, il vigente D.Lgs. n. 196/2003, e i provvedimenti emanati nel tempo dal Garante per la protezione dei dati personali e le altre istituzioni nazionali ed europee competenti in materia.
In particolare, il documento regolamenta:

a) i **ruoli e le responsabilità** assegnate ai vari livelli gestionali, di controllo e operativi, al fine di garantire la corretta tenuta del predetto modello e, di conseguenza, la conformità alla normativa di riferimento;
b) le modalità per il rilascio delle necessarie **istruzioni** ai soggetti autorizzati, ai vari livelli, al trattamento dei dati personali;
c) gli strumenti per il **monitoraggio e controllo** del sistema, al fine di garantire il miglioramento continuo dello stesso e il mantenimento della conformità alla normativa vigente.

Il presente documento è portato a conoscenza, anche attraverso attività di sensibilizzazione o formazione, a tutti i dipendenti dell'Azienda.

RIFERIMENTI NORMATIVI

1. Titolare del trattamento (art. 4, n. 7 e art. 24 del GDPR);
2. Responsabile della Protezione dei Dati (art. 37 e ss. del GDPR);
3. Soggetti che trattano dati "per conto" e sotto l'autorità del Titolare del trattamento (art. 29 del GDPR);
4. Attribuzione di funzioni e compiti a soggetti designati (art. 2-quaterdecies del D.Lgs. n. 196/2003);
5. Garante per la protezione dei dati personali, Comunicato 11 dicembre 1997 "Privacy: chi sono i titolari e i responsabili del trattamento dei dati nelle imprese e nelle amministrazioni pubbliche";
6. Linee Guida EDPB 7/2020 sui concetti di Titolare e Responsabile del Trattamento;
7. Garante per la protezione dei dati personali, Provvedimento del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" e s.m.i.;
8. Decisione della Commissione UE 2021/915 del 4 giugno 2021, recante le clausole tipo dell'atto che regola il rapporto tra Titolare e Responsabile del Trattamento.

CONTESTO ORGANIZZATIVO DI RIFERIMENTO

La struttura dell'Azienda speciale è definita dallo Statuto, oltre che da atti Macro e Micro Organizzazione assunti dal CDA e dal Direttore nell'ambito delle rispettive competenze.

La struttura aziendale è articolata nei seguenti livelli di responsabilità, primari, secondari, di base: direzione – staff della direzione – settori.

L'assetto delle responsabilità in materia di trattamento e gestione dei dati personali si conforma alla struttura propria della Azienda come risultante dal delineato sistema organizzativo interno.

Con il presente Regolamento è definito il contenuto specifico delle responsabilità in materia di trattamento e gestione dei dati personali. (…..) ed è delineato, nell'ambito della più generale *governance* dell'Ente, il Modello Organizzativo Privacy (MOP), caratterizzato da una articolazione **"a rete"** di funzioni e competenze di gestione e controllo in materia di *privacy compliance*.

In tale contesto, i processi coordinati a livello centrale dal Titolare del trattamento, coadiuvato dal Responsabile della Protezione dei Dati (RPD), trovano attuazione all'interno della Struttura organizzativa dell'Ente attraverso:

a) un livello dirigenziale, proprio del Direttore, con autonomia gestionale e organizzativa, che riferisce direttamente al Titolare; il Direttore assume il ruolo di **Delegato del Titolare o Delegato Privacy**, ed è da considerare soggetto designato ai sensi dell'art. 2-quaterdecies, co. 1 del D.Lgs. 196/2003, per effetto della documentata preposizione alla direzione; allo stesso sono affidati specifici compiti e funzioni connessi al trattamento dei dati personali di competenza successivamente delineati;
b) la nomina del **Responsabile della protezione dei dati (RPD/DPO)**, con funzioni di supporto al Titolare del trattamento e di monitoraggio e controllo del sistema implementato;
c) l'individuazione di uno o più **Referenti Privacy** che supportano il RPD nell'affrontare le questioni connesse alla sicurezza e alla gestione dei dati personali per la corretta applicazione del regolamento europeo, partecipando a tal fine agli appositi incontri periodici e riferendo direttamente al vertice dirigenziali dell'Ente;
d) i meccanismi e le modalità per **l'identificazione e autorizzazione degli ulteriori soggetti responsabili**, che effettuano i trattamenti di dati personali, sotto la diretta autorità del Titolare e del Delegato di cui alla precedente lett. a), come segue: i Responsabili di Staff, quali "Autorizzati Responsabili"; gli altri dipendenti, quali "Autorizzati".

A tali soggetti interni si aggiungono i Responsabili del Trattamento, soggetti esterni all'Amministrazione individuati dal Titolare con proprio provvedimento cui accede apposito contratto.

RUOLI E RESPONSABILITA'

TITOLARE DEL TRATTAMENTO

L'interpretazione da sempre avallata dal Garante per la protezione dei dati personali prevede che il meccanismo di imputazione delle responsabilità in materia di privacy sia mutuato dallo schema organizzativo in concreto adottato dall'ente con riguardo alle potestà decisionali.

In linea con tale interpretazione e ferma restando la qualifica di *Titolare del trattamento* da **identificarsi nella struttura nel suo complesso e, quindi, in capo all'Azienda speciale,** le funzioni di natura gestionale che la legge attribuisce al *Titolare*, non possono che essere originariamente individuate in capo al **Consiglio di Amministrazione**.

In tal senso, si ritiene che il CDA, in materia, debba determinare - considerando la natura, l'ambito di applicazione, il contesto, i rischi per i diritti e le libertà degli interessati - le finalità e le modalità del trattamento, assicurando che venga adottato un sistema di gestione degli adempimenti privacy e adeguate misure di sicurezza, in conformità ai requisiti del Regolamento UE e ai principi di accountability (affidabilità e responsabilizzazione) e di privacy by design & by default (adozione di misure tecniche e organizzative adeguate per la protezione - trattamento dati per impostazione predefinita).

In considerazione di tali funzioni, il Consiglio provvede:

a) a nominare il Responsabile della Protezione dei Dati (RPD/DPO);
b) a nominare, anche mediante delega al Direttore, i Responsabili del Trattamento laddove ne ricorrano i presupposti;
c) ad approvare, anche mediante delega al Direttore, i principali documenti gestionali per il regolare ed efficiente funzionamento del sistema privacy ovvero:
   - ✓ il presente modello organizzativo;
   - ✓ il Registro dei Trattamenti;
   - ✓ la procedura di gestione dei data breach;
   - ✓ gli altri documenti a carattere generale.
d) a conferire espressa delega, considerandosi tale anche quanto attribuito con il presente MOP, al Direttore per la gestione dei vari adempimenti rilevanti, anche per rinvio alle funzioni previste dal presente atto;
e) ad adottare tutte le decisioni che eventualmente non rientrino nelle competenze ordinarie e nei limiti di spesa del Direttore;
f) a riesaminare e aggiornare periodicamente, avvalendosi del Responsabile della Protezione che riferisce direttamente al Titolare, le misure a tutela degli interessati ai fini della *compliance* generale dell'Ente al GDPR.

RESPONSABILE DELLA PROTEZIONE DEI DATI

Nel rispetto di quanto previsto dall'art. 37 del Reg. 2016/679, il Responsabile della Protezione Dati è nominato dal CDA, anche tra i dipendenti aziendali, e fino a diversa sua disposizione.

Il RPD è individuato in funzione delle qualità professionali e, in particolare, della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, nonché della capacità di assolvere i compiti di legge.

Il RPD costituisce presso l'Azienda una figura di riferimento per tutte le questioni di carattere generale riguardanti la protezione dei dati personali.

Al RPD dell'Azienda sono affidati i seguenti compiti:

a) supportare, informare e fornire consulenza al Titolare (in tutte le sue articolazioni) e ai Responsabili del Trattamento nel percorso di implementazione del GDPR a livello organizzativo e gestionale, nonché per l'applicazione delle adeguate misure di sicurezza per la corretta gestione dei dati personali e per la definizione di eventuali misure più idonee di cui sia indispensabile programmare l'implementazione;
b) sovraintendere alla tenuta del Registro dei Trattamenti di cui all'art. 30 del GDPR, coordinando, con la piena collaborazione del Delegato e del Referente, le attività di compilazione da parte dei soggetti Autorizzati Responsabili e Autorizzati, e consolidando il Registro - previa verifica del rispetto delle regole impartite dal Titolare - con la creazione di versioni consequenziali, ordinate cronologicamente;
c) esprimere, se richiesto, formale parere sui documenti di carattere gestionale (es., configurazione delle responsabilità interne, procedure, linee guida, istruzioni formalizzate ai soggetti autorizzati) e sulle adeguate misure di sicurezza che sono o verranno proposte per la gestione dei dati personali della Azienda;
d) informare e fornire consulenza al Titolare (in tutte le sue articolazioni), ai Responsabili del Trattamento e ai dipendenti sui loro obblighi derivanti dal GDPR e da altre vigenti disposizioni; in questo ambito, al RPD potrà essere richiesto di partecipare a incontri operativi ai vari livelli nell'ambito degli organi di governance della Azienda in cui vengano assunte decisioni relative al trattamento dei dati personali;
e) sorvegliare e valutare l'osservanza del RGPD e le politiche interne in materia di protezione dei dati personali, compresi gli strumenti e le attività realizzate per la sensibilizzazione e la formazione del personale, anche attraverso la conduzione di audit e visite ispettive programmate e/o a sorpresa;
f) fornire, se richiesto, un parere sulla valutazione d'impatto del trattamento sulla protezione dei dati di cui agli artt. 35 e ss. del RGPD, in particolare: valutando le metodologie utilizzate, provvedendo a esaminarne gli esiti finali e supportando le decisioni connesse agli eventuali obblighi di consultazione preventiva del Garante della protezione dei dati personali;

g) partecipare alle istruttorie e valutazioni circa eventuali violazioni di dati personali occorsi presso l'Azienda, supportando il soggetto competente - secondo quanto previsto dal Regolamento sulla gestione degli incidenti - nelle decisioni circa:
   - la gestione delle notificazioni e comunicazioni dei data breach di cui agli artt. 33 e 34 del RPGD;
   - la segnalazione di tali violazioni a eventuali Contitolari o Titolari autonomi, secondo le istruzioni contrattualmente definite;

h) provvedere alla alimentazione e aggiornamento del Registro dei data breach;

i) cooperare con il Garante per la protezione dei dati personali (o altra Autorità di controllo competente) e fungere da punto di contatto per facilitare l'accesso, da parte di questa, ai documenti e alle informazioni necessarie ai fini dell'esercizio dei poteri di indagine, correttivi, autorizzativi e consultivi alla stessa attribuite dal RGPD;

j) fungere da punto di contatto e curare i rapporti con gli interessati, per il tramite e con la collaborazione diretta dei responsabili di Area/Ufficio/processo competenti, rispetto alla materia oggetto della questione con l'interessato, nell'analisi ed evasione di ogni questione che venga sottoposta direttamente alla propria attenzione ovvero all'attenzione del Titolare del trattamento e alimentando il Registro delle richieste di esercizio dei diritti degli interessati;

k) fornire inoltre il suo apporto alla verifica della funzionalità del programma di formazione e istruzione funzionale del personale aziendale; se del caso potrà svolgere attività di formazione introduttiva al personale sulle principali tematiche del RGPD;

l) tenere l'elenco dei Responsabili del Trattamento;

m) provvedere alla istituzione, alimentazione e aggiornamento del Registro delle richieste di esercizio dei diritti degli interessati.

I compiti del Responsabile della Protezione dei Dati attengono all'insieme dei trattamenti di dati effettuati dall'Azienda e comprendono:

a) l'attività eventualmente delegata a soggetti esterni;

b) la vigilanza su eventuali trattamenti svolti, su incarico dell'Azienda, da società in house del Sistema camerale e in tutti i casi di attribuzione di Responsabilità del trattamento.

Il RPD, in relazione all'esercizio delle proprie funzioni e dei relativi compiti è tenuto:

a) a stringenti vincoli di riservatezza nel trattamento dei dati personali/informazioni acquisite; tale vincolo non opererà in relazione agli obblighi connessi a eventuali richieste formalizzate da Pubbliche autorità con funzioni inquirenti, giudicanti e di controllo;
b) a comunicare immediatamente eventuali situazioni di conflitti d'interesse sopravvenuti ovvero l'insorgenza di una delle situazioni che costituiscono causa di decadenza dell'incarico;
c) ad adempiere ai compiti affidati con la diligenza richiesta dalla natura dell'incarico stesso, dalla natura dell'attività esercitata e dalle specifiche competenze detenute, garantendo un

atteggiamento leale nello svolgimento del proprio ruolo ed evitando, con la propria azione o con la propria inerzia, di causare problematiche o criticità non riconducibili al rigoroso adempimento degli obblighi di supporto o vigilanza connessi al ruolo.

Il RPD riferisce:

- ordinariamente al Direttore, anche per il tramite del Referente, in qualità di vertice organizzativo dell'Ente e, quindi, in grado di intervenire tempestivamente in caso di criticità rilevate.
- periodicamente al CDA, mediante la formalizzazione della reportistica ovvero esprimendo le sue valutazioni quando lo riterrà opportuno o si renderà necessario, o quando gli verrà espressamente richiesto.

Il RPD potrà essere convocato dal CDA, compatibilmente con le sue esigenze di servizio o personali, per riferire in merito al funzionamento del sistema di gestione dei dati personali o a situazioni specifiche.

Al fine di garantire i necessari requisiti di autonomia e indipendenza nell'esecuzione dell'incarico, per effetto dell'approvazione del presente modello, al RPD sono attribuiti i seguenti poteri e prerogative, in assenza di qualsivoglia istruzione (come stabilito dall'art. 38, comma 3, GDPR):

a) l'Azienda gli mette a disposizione, al fine di consentire l'ottimale svolgimento dei compiti e delle funzioni assegnate, adeguate risorse economiche, strumentali e umane, con particolare riferimento a una idonea postazione di lavoro in grado di garantire la funzionalità delle attività e la riservatezza che deve caratterizzare il loro svolgimento, nonché la necessaria strumentazione informatica per la normale operatività in loco, e compreso uno o più "Referenti Privacy", con il compito di supporto giuridico-amministrativo del RPD nelle attività che esso dovrà svolgere, e un referente ICT (Tecnologie dell'informazione e della comunicazione) che dovrà supportare operativamente il RPD in tutte le attività di valutazione, analisi e indicazioni legate all'infrastruttura e agli applicativi informatici e telematici in uso presso l'ente, rendendo disponibile, a tal fine, il servizio di assistenza tecnica di InfoCamere;

b) l'Azienda non potrà rimuovere o penalizzare il RPD in ragione dell'adempimento dei compiti affidati nell'esercizio delle sue funzioni e garantisce che il RPD eserciterà le proprie funzioni in autonomia e indipendenza, non potendo assegnare allo stesso attività o compiti che risultino in contrasto o conflitto di interesse;

c) il RPD deve essere coinvolto, tempestivamente e adeguatamente, da parte della Azienda, in tutte le questioni che riguardano la protezione dei dati personali sin dalle fasi iniziali, fornendo il quadro completo di tutte le informazioni pertinenti;

d) al RPD è garantita, da parte della governance e di tutto il personale, la dovuta considerazione, con particolare riferimento ai pareri e alle indicazioni fornite;

e) l'Azienda deve mettere a disposizione una specifica casella di posta elettronica che sarà utilizzata per tutte le comunicazioni ufficiali in ingresso e uscita, nonché quale dato di contatto per il Garante per la protezione dei dati personali e per gli interessati;

f) i dati di contatto del RPD (recapito postale, telefono, email), comunicati al Garante per la protezione dei dati personali, sono resi disponibili, a esclusione del suo nominativo, sul sito internet istituzionale della Azienda, e riportati nelle informative rese agli interessati;

g) al RPD sono inoltre riconosciuti, per effetto del presente atto:
- potere di autoregolamentazione, in forza del quale il RPD potrà programmare autonomamente le proprie attività, garantendo comunque l'assolvimento dei compiti precedentemente indicati e rendendo conto delle attività effettivamente espletate ai fini della verifica di idoneità ed efficace attuazione del sistema privacy implementato rispetto agli obblighi di cui al GDPR;
- poteri ispettivi, in forza dei quali, nell'esercizio delle proprie funzioni di controllo, il RPD potrà:
  a) utilizzare le risultanze delle attività ispettive e svolgere autonomamente verifiche anche a sorpresa;
  b) accedere liberamente a ogni documento rilevante per lo svolgimento delle sue funzioni;
  c) disporre l'acquisizione di informazioni, dati e/o notizie a semplice richiesta, senza preventiva autorizzazione;
  d) richiedere l'audizione ovvero il coinvolgimento nelle attività di verifica di qualsivoglia dipendente dell'Ente;
  e) esercitare i poteri, come precedentemente esplicitato, anche nei confronti delle società in house del sistema camerale, quando svolgano le funzioni di Responsabili esterni del trattamento (in questi casi, affiancando il dirigente competente).

DELEGATO DEL TITOLARE DEL TRATTAMENTO - DIRETTORE

Ai seguenti soggetti, ai sensi dell'art. 2-quaterdecies, comma 1, del D.Lgs. n. 196/2003 e in forza dei poteri statutari e delle deleghe gestionali conferite, è assegnata, in materia di privacy, al Direttore, coerentemente con le competenze statutarie, la gestione delle funzioni delegate di seguito descritte:

a) sottoscrizione degli accordi di contitolarità con enti e istituzioni minori (a titolo di esempio Istituti scolastici, Organismi di Mediazione e Arbitrato);
b) sottoscrizione degli accordi di contitolarità con le principali e strategiche Istituzioni e Autorità nazionali, regionali e comunali (come per esempio, Ministeri e Autorità Indipendenti, Regione, Provincia, Comuni di Cagliari e Oristano e loro Assessorati o Agenzie, Autorità Portuale, Camere di commercio), solo su delega espressa e specifica da parte del CDA, e previa approvazione da parte dello stesso anche del relativo accordo di contitolarità;
c) approvazione con propria determinazione del Registro dei Trattamenti con individuazione di apposite regole per la sua tenuta e per il suo periodico aggiornamento;

d) aggiornamento e manutenzione, con propria determinazione, dei documenti gestionali approvati dal CDA in funzione delle modifiche normative e organizzative eventualmente intervenute e all'emergere di eventuali criticità o necessità di miglioramento gestionale;
e) predisposizione e approvazione di eventuali documenti operativi (es., linee guida, procedure, istruzioni operative, format di informative e consensi, etc.) del sistema di gestione che si rendessero necessari per garantire la più efficace implementazione dei requisiti del GDPR;
f) sottoscrizione delle notifiche dei data breach e approvazione delle comunicazioni agli interessati, secondo quanto previsto da apposita procedura gestionale;
g) garanzia che i dati personali oggetto del trattamento siano trattati in modo lecito e secondo correttezza, nel rispetto delle disposizioni contenute nel Regolamento (UE) 2016/679 e nei provvedimenti del Garante della Privacy applicabili, nonché nel rispetto di eventuali istruzioni che saranno fornite dal Titolare: deve dare disposizione che i dati personali siano raccolti e registrati per scopi inerenti alle funzioni istituzionali dell'ente, che gli uffici verifichino che i dati siano esatti, completi, non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati, e che siano conservati rispettando le misure di sicurezza predisposte dall'Azienda;
h) attuazione delle misure tecniche e organizzative adeguate al fine di garantire un livello di sicurezza idoneo rispetto al rischio, tenendo conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati;
i) indicazione della necessità di predisporre misure di sicurezza più efficaci o alternative rispetto alle pre-esistenti, non solo in caso di rilevante modifica normativa di settore;
j) gestione degli adempimenti derivanti dall'esercizio dei diritti degli interessati (artt. 15 e ss. del GDPR) e/o dai reclami, ovvero relativi a processi o fasi di attività ricadenti nella propria diretta competenza, attivandosi per alimentare il "Registro delle richieste di esercizio dei diritti degli interessati", e fornendo supporto al RPD ove la richiesta sia pervenuta direttamente a lui ovvero in fase di "riesame" della risposta formalizzata all'interessato, ove richiesto;
k) approvazione, sentito il RPD, di percorsi formativi e strumenti informativi periodici, al fine di definire necessarie istruzioni al personale;
l) controllo sull'attività svolta dalle persone autorizzate al trattamento al fine di verificare l'effettivo rispetto da parte di questi delle misure di sicurezza adottate e delle istruzioni impartite;
m) utilizzo delle informative;
n) supporto al Garante in caso di richiesta di informazioni o di controlli relativi alla protezione dei dati;
o) proposta in caso di cessazione del trattamento delle modalità di dismissione delle banche dati (distruzione- cessione – conservazione definitiva) secondo le formalità di legge;
p) affidamento incarichi di Responsabile del Trattamento dei dati e definizione e sottoscrizione delle clausole contrattuali o atti giuridici analoghi per il conferimento delle relative responsabilità (art. 28);

q) accettazione di incarichi di Responsabile del Trattamento da parte della Azienda, conferiti da parte di altri Titolari, laddove sia funzionale alla erogazione dei servizi all'utenza, e regolati da apposito atto;
r) istruzioni ai soggetti autorizzati sottoposti alla sua diretta responsabilità;
s) nomina degli Amministratori di Sistema;
t) gestione dei flussi informativi al RPD, come definiti nell'apposito paragrafo del presente documento, e più in generale comunicazione allo stesso di ogni notizia rilevante ai fini della protezione dei dati personali e degli interessati.

REFERENTI PRIVACY

I Referenti privacy sono dipendenti della Azienda, nominati dal Direttore e individuati in funzione delle qualità professionali che permettano di prestare adeguato supporto al RPD nell'esecuzione dei suoi compiti.

Essi, vigilano che la diffusione dei dati personali (diversi da quelli sensibili e giudiziari che risulta allo stato essere vietata) avvenga solo se prevista da specifica normativa (ad es., con riferimento agli obblighi di pubblicazione per finalità di pubblicità integrativa dell'efficacia e di trasparenza, ai sensi del D.Lgs. 33/2013 e s.m.i.).

Si attivano - in collaborazione con il RPD - per fare in modo che, in relazione ad ogni nuova iniziativa o progetto che comporti un trattamento di dati personali, sia effettuata una verifica preventiva della liceità e della legittimità del trattamento, nonché delle modalità con le quali si intende eseguirlo; ove necessario, sulla base degli artt. 35 e 36 del Regolamento e delle Linee guida europee e del Garante, provvedono a eseguire, in collaborazione con il RPD, la valutazione d'impatto sulla protezione dei dati e a supportare il Titolare nell'attivazione della consultazione preventiva del Garante ove ritenuta necessaria.

Sollecitano l'adozione da parte dell'Azienda delle misure preventive e correttive connesse, ad es., all'organizzazione interna del lavoro, alla gestione di eventuali fornitori e strumenti informatici, ai flussi informativi e documentali di competenza.

SOGGETTI AUTORIZZATI AL TRATTAMENTO

L'art. 4, punto 10, del Regolamento UE prevede espressamente la figura delle *"persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile"*.

I soggetti autorizzati, ai sensi dei successivi articoli 29 e 32, comma 4, del Regolamento UE, non possono trattare i dati personali se non sono istruiti in tal senso dal Titolare del trattamento, atteso che le istruzioni rientrano tra le idonee misure che devono essere assunte per garantire un adeguato livello di sicurezza nella protezione dei dati.

Il D.Lgs. n. 196/2003, come modificato dal D.Lgs. n. 101/2018, inoltre, lascia ampia scelta al Titolare del trattamento nel definire le modalità ritenute più idonee per autorizzare al trattamento i soggetti che operano sotto la propria autorità diretta.

Pertanto, il Delegato Privacy (Direttore) provvede ad autorizzare, i Responsabili di Staff quali "Autorizzati Responsabili", e i restanti dipendenti aziendali quali "Autorizzati", e assegna loro specifiche istruzioni che devono avere come contenuto minimo quelle indicate nel presente Regolamento.

Tutti i dipendenti aziendali si considerano, in automatico, in forza del presente Regolamento, e secondo gli ordini di servizio che dispongono la mobilità interna, soggetti "Autorizzati", con dovere di rispettare le istruzioni contenute nello stesso Regolamento.

AUTORIZZATI RESPONSABILI - RESPONSABILI DI STAFF E DI SETTORE

I Responsabili di Staff e di Settore si qualificano come "Autorizzati Responsabili".

Essi applicano la normativa di riferimento e rispettano le istruzioni definite dal Titolare in collaborazione con il RPD attraverso i documenti gestionali del sistema privacy, provvedendo ad adattare, secondo le specifiche necessità di volta in volta emergenti nell'ambito della attività di competenza, i format e i modelli contenuti nei regolamenti generali adottati per la gestione degli adempimenti in materia privacy dalla Azienda.

Gli Autorizzati Responsabili, pertanto, sono destinatari di ogni comunicazione concernente l'adozione da parte dell'Ente di atti di carattere generale come regolamenti, procedure, circolari, linee guida, provvedimenti adottati dalla Azienda in materia di privacy.

Essi verificano le esigenze di integrazione o aggiornamento dei predetti atti, evidenziando, ad esempio, al Direttore e al RPD le eventuali necessità di modifica/integrazione del Registro dei Trattamenti di cui all'art. 30 del Regolamento, in relazione, a puro titolo esemplificativo, a:

- esigenze derivanti da nuovi servizi/progetti diversi o nuovi rispetto a quelli attualmente censiti;
- modifiche organizzative interne che comportino diverse modalità di gestione dei trattamenti di dati, anche ai fini dell'analisi dei rischi (ad es., acquisizione di applicativi informatici per la gestione di determinate attività rientranti nella propria autonomia gestionale).

Gli Autorizzati Responsabili, inoltre, per quanto di competenza:

- collaborano con il RPD nelle attività di impulso volte ad alimentare il Registro dei Trattamenti, raccogliendo presso i diversi settori le informazioni a tal fine necessarie.
- rilevano e segnalano al Direttore le eventuali e specifiche esigenze formative o di approfondimento da considerare ai fini della progettazione e programmazione dei percorsi formativi interni.

Ai soggetti Autorizzati Responsabili sono assegnati compiti di controllo e monitoraggio sul rispetto da parte degli Autorizzati delle istruzioni ricevute e del dovere di riservatezza.

AUTORIZZATI - DIPENDENTI

I soggetti Autorizzati svolgono i trattamenti "per conto" del Titolare e sono formalmente autorizzati anche per relationem con rinvio al presente Regolamento e al Registro dei Trattamenti.

Tutto il personale Autorizzato (compresi gli Autorizzati-Responsabili) deve effettuare le operazioni di trattamento secondo le seguenti istruzioni del Titolare:

1) accedere ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati facendo riferimento alla specifica scheda analitica del Registro dei Trattamenti per l'individuazione degli elementi fondamentali dei trattamenti che si è autorizzati a effettuare;
2) garantire la massima riservatezza su qualsiasi informazione e dato personale di cui vengano a conoscenza nell'esercizio delle proprie funzioni, in conformità a quanto previsto normativamente in tema di segreto d'ufficio e di segreto d'impresa, non comunicandoli a terzi in alcun modo se non nei casi espressamente previsti, e non utilizzandoli per altri fini;
3) trattare i dati in modo lecito, corretto e trasparente, raccogliendoli per finalità legittime e trattandoli in modo che non vi sia incompatibilità con tali finalità, acquisendo solo dati adeguati, pertinenti e non ridondanti rispetto alle finalità, in attuazione del principio di minimizzazione dei dati, ed esatti e aggiornati, provvedendo a semplice richiesta, previa verifica, o d'ufficio, alla cancellazione o rettifica dei dati inesatti;
4) fornire all'interessato l'informativa secondo i modelli adottati, conservandone, ove ritenuto opportuno, copia controfirmata per ricevuta di avvenuta consegna;
5) conservare i dati personali raccolti per un periodo non superiore a quello indicato dal Titolare in base alla vigente normativa e provvedere periodicamente, a norma di legge, alla cancellazione dei dati personali per i quali non sussistono ragioni di fatto o di diritto che ne giustificano la conservazione;
6) custodire i dati personali raccolti con la massima diligenza, escludendo dall'accesso tutti coloro che non sono autorizzati, e tenendo, a tal fine, gli atti, i documenti e i supporti informatici contenenti dati personali in armadi muniti di serratura; qualora gli armadi in dotazione all'ufficio non fossero disponibili o sufficienti informare per iscritto il diretto superiore;
7) valutare l'opportunità di tenere archivi separati per la conservazione di dati particolari;
8) riferire al responsabile di eventuali richieste di accesso ai documenti amministrativi che comportino la conoscenza di dati personali di terzi;
9) seguire obbligatoriamente i percorsi formativi che saranno organizzati dall'Ente;
10) rispettare le disposizioni impartite per iscritto dal Titolare o dal Delegato del Titolare attraverso la documentazione rilevante a fini privacy, nonché tutte le ulteriori istruzioni che saranno dagli stessi soggetti formalizzate;

11) utilizzare le misure di sicurezza per la protezione fisica, informatica e telematica dei dati personali secondo le specifiche istruzioni definite nell'ambito del sistema di gestione privacy, con particolare riferimento al controllo e custodia degli atti e dei documenti contenenti dati personali per evitare visione, possesso, utilizzo non autorizzati da parte di terzi, compresi i dipendenti di altri uffici o servizi aziendali; in particolare è doveroso:
    - custodire con la massima diligenza le credenziali di autenticazione al fine di assicurarne la totale segretezza, potendole comunicare esclusivamente ad altro dipendente dello stesso ufficio per i soli casi di necessità, ossia solo se dalla omessa comunicazione possa derivare una interruzione del servizio che l'Ente deve erogare, e avendo cura di modificarle prontamente una volta venuto meno lo stato di necessità;
    - adottare password di almeno otto caratteri di cui almeno due numerici, senza riferimenti riconducibili agevolmente ai dati anagrafici propri o dei propri familiari, e modificarle almeno ogni sei mesi;
    - non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento;
    - utilizzare esclusivamente software reso disponibile dall'ente;
    - non collegare modem o dispositivi che consentano un accesso non controllato al computer o alla rete;
    - non rimuovere il sistema antivirus installato sul computer;
    - in caso di utilizzo di supporti removibili verificarne sempre preliminarmente l'integrità a mezzo del programma antivirus installato;
    - non scaricare file eseguibili o documenti di testo da siti internet senza verificare l'assenza di virus;
    - attivare una password di screensaver per evitare accessi non autorizzati al computer quando la postazione non è presidiata;
    - non condividere il proprio hard disk con altro computer salvo ciò non sia richiesto da ragioni organizzative imposte per iscritto dall'amministrazione;
12) comunicare al RPD, attraverso il Delegato, ogni notizia rilevante ai fini della protezione dei dati personali e degli interessati; qualora ne venga a conoscenza nell'espletamento delle attività di competenza o indirettamente nello svolgimento delle stesse, informare tempestivamente (possibilmente entro il limite di 24 ore dal momento in cui si viene a conoscenza del fatto) il RPD, attraverso il Delegato/Referente privacy, del verificarsi di eventuali violazioni dei dati personali che possano esporre a rischio le libertà e i diritti degli interessati ovvero la sicurezza, integrità e disponibilità dei dati trattati (data breach);
13) collaborare più in generale con il RPD provvedendo a fornire ogni informazione da questi richiesta.

Le istruzioni sopra elencate sono quelle minime da rispettare. I soggetti Autorizzati Responsabili possono proporre al Direttore l'adozione di ulteriori istruzioni in relazione agli specifici trattamenti curati dal settore di competenza. Il Delegato può dunque integrare le istruzioni sopra elencate per le specifiche esigenze dell'Azienda o di uno specifico settore.
Qualora si rendesse necessario derogare o modificare le istruzioni minime in parola, tutti gli Autorizzati dovranno darne apposita motivazione e puntuale giustificazione.

Il mancato rispetto delle istruzioni impartite a tutela della privacy potrebbe comportare l'insorgere di responsabilità dell'Azienda con conseguente possibile contestazione disciplinare, in base al vigente CCNL, a carico del dipendente.

AMMINISTRATORI DI SISTEMI

Il Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" e s.m.i. definisce l'amministratore di sistema come la *«figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise resource planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali»*.

I soggetti che svolgono funzioni di amministrazione di sistemi (ad es., addetti alla gestione e manutenzione di un impianto di elaborazione o di sue componenti; amministratori di basi di dati; amministratori di reti e di apparati di sicurezza, amministratori di applicativi complessi):

✓ sono "responsabili" di specifiche fasi lavorative ovvero di strumenti che possono comportare elevate criticità rispetto alla protezione dei dati;
✓ pur non essendovi preposti istituzionalmente, possono anche "solo incidentalmente" trovarsi nella necessità di trattare dati personali ai soli fini dell'espletamento delle loro consuete attività.

Il Provvedimento del Garante definisce gli adempimenti da formalizzare sia in relazione ai dipendenti che svolgano tali funzioni sia nel caso di servizi affidati in outsourcing.

In attuazione di tale provvedimento, l'Azienda procede alla nomina dei necessari Amministratori di Sistema, i cui compiti, specificatamente e limitatamente a tale contesto, consistono in:

- assicurare la corretta custodia delle credenziali per la gestione dei sistemi di autenticazione e di autorizzazione in uso in ambito aziendale, anche impartendo apposite istruzioni agli incaricati del trattamento che utilizzino strumenti elettronici;
- predisporre e rendere funzionanti le copie di sicurezza (operazioni di *backup* e *disaster recovery*) dei dati e delle applicazioni;
- predisporre sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici, nella sua qualità di "amministratore di sistema"; tali registrazioni (access log) devono essere effettuate in modo da avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste;

- relazionare, periodicamente, circa l'attività svolta e lo stato di attuazione delle politiche in tema di protezione dei dati personali, segnalando eventuali criticità.

RESPONSABILI DEL TRATTAMENTO

A norma dell'art. 28 del Regolamento UE, l'Azienda può incaricare, quali Responsabili del Trattamento, persone fisiche, enti e società che trattano i dati per suo conto.

Possono essere incaricati unicamente soggetti in possesso di requisiti di esperienza, capacità ed affidabilità tali da fornire idonea garanzia del rispetto delle disposizioni stabilite nel Regolamento UE, ivi compreso il profilo della sicurezza, ossia la capacità di mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento garantisca la tutela dei dati personali di cui l'Azienda è Titolare.

L'incarico come Responsabile può essere disposto o direttamente dal Titolare, con deliberazione di CDA, o dal Delegato-Direttore, con propria determinazione. In tal caso, il Delegato informa il CDA nella prima riunione successiva, al fine di consentire al Titolare l'esercizio della facoltà di opporsi, con applicazione dell'istituto del silenzio-assenso.

I trattamenti effettuati da un Responsabile sono disciplinati da un contratto/atto collegato all'atto che vincola il Responsabile stesso al Titolare del trattamento e che definisce la materia disciplinata e la durata del trattamento, la natura e la finalità, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

L'atto di incarico dovrà contenere le seguenti indicazioni:

- il tipo di dati trattati;
- la natura e la finalità del trattamento;
- le categorie di interessati;
- la precisazione che le informazioni di dettaglio, relative a ciascun trattamento affidato dal Titolare al Responsabile, sono descritte nel proprio "Registro dei Trattamenti" informatico che costituisce parte integrante dell'atto di nomina e che sarà aggiornato dal Responsabile per le attività di propria competenza, consentendo eventuale visibilità al Titolare di tutte le informazioni necessarie affinché questo possa esercitare il controllo sui trattamenti affidati;
- la durata che deve essere pari al periodo per il quale i trattamenti dei dati sono affidati al Responsabile prescelto;

Lo stesso atto di incarico, alla luce della Decisione UE 2021/915, dovrà, inoltre, prevedere, quale contenuto minimo, le prescrizioni e gli obblighi appresso indicati:

- l'obbligo del Responsabile di comunicare prontamente al Titolare eventuali situazioni sopravvenute che, per il mutare delle conoscenze acquisite in base al progresso tecnico

o per qualsiasi altra ragione, possano incidere sulla propria idoneità allo svolgimento dell'incarico.

- il Responsabile, dovrà svolgere il trattamento dei dati personali per le finalità e secondo le modalità stabilite, in ogni momento, dal Titolare del trattamento e, dovrà, comunque, attenersi alle istruzioni documentate impartitegli dallo stesso Titolare con l'apposito atto di affidamento incarico, fatti salvi i trattamenti effettuati per obbligo di legge cui è soggetto il Responsabile del trattamento in base al diritto interno a europeo; in tal caso, il Responsabile del trattamento informa il Titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto lo vieti per rilevanti motivi di interesse pubblico;

- il Responsabile dovrà seguire le seguenti istruzioni:

1. effettuare il trattamento dei dati personali in modo lecito e secondo correttezza nel rispetto delle istruzioni del Titolare, delle disposizioni contenute nel Regolamento UE 2016/679, e nei provvedimenti del Garante della Privacy applicabili;
2. concedere l'accesso ai dati personali oggetto di trattamento al suo personale soltanto nella misura strettamente necessaria per l'attuazione, la gestione e il controllo del servizio affidato e del presente atto;
3. impartire alle persone autorizzate al trattamento dei dati personali, dipendenti o collaboratori del Responsabile, il dovere, con rilevanza di obbligo legale, di riservatezza dei dati e del rispetto della normativa vigente e dei provvedimenti del Garante applicabili, e impartire, altresì, la necessaria formazione, comprensiva delle necessarie e opportune istruzioni;
4. adottare tutte le necessarie e appropriate misure di sicurezza tecniche e organizzative così come disciplinate dal Regolamento UE, e ciò include la protezione da ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati (violazione dei dati personali), tenendo debitamente conto, nel valutare l'adeguato livello di sicurezza, dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi per gli interessati; al qual proposito, il Responsabile garantisce, e il Titolare ne prende atto, di essere dotato di un proprio Sistema di gestione della sicurezza delle informazioni in costante aggiornamento in relazione allo stato del progresso tecnico;
5. provvedere, in particolare e in modo concreto, ad attivare le seguenti misure minime di sicurezza tecniche e organizzative:
   - effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema informatico usato;
   - per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati;
   - effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore;
   - verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova;
   - assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura;

- assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza;
- segnalare al Titolare del trattamento eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle misure di sicurezza adottate al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;

6. adottare, inoltre, le seguenti misure organizzative da verificare periodicamente nella loro efficacia al fine di garantire la sicurezza del trattamento da parte degli incaricati:
   - assicurare la formazione delle persone autorizzate al trattamento;
   - attuare un controllo sulla loro attività al fine di verificare l'effettivo rispetto da parte di questi ultimi delle misure di sicurezza adottate e, comunque, delle istruzioni impartite;
   - impartire agli incaricati le seguenti istruzioni:
     i. quando appositamente autorizzato all'accesso alle banche dati informatiche, custodire con attenzione le proprie credenziali di autenticazione e ogni dispositivo che le contiene, ed evitare di operare su terminali altrui e/o di lasciare accessibile il sistema operativo in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati;
     ii. trattare i soli dati la cui conoscenza sia necessaria e sufficiente per lo svolgimento delle operazioni da effettuare;
     iii. conservare i supporti informatici e/o cartacei contenenti i dati personali, in modo da evitare che siano accessibili a persone non autorizzate al trattamento dei dati medesimi o siano facilmente oggetto di danneggiamenti intenzionali o accidentali;
     iv. con specifico riferimento agli atti e documenti cartacei contenenti dati personali e alle loro copie, restituire gli stessi al termine delle operazioni affidate;
     v. copie di dati personali oggetto di trattamento devono essere effettuate esclusivamente se necessario e soltanto previa autorizzazione del titolare del trattamento;
     vi. in caso si constati o si sospetti un incidente di sicurezza deve essere data immediata comunicazione al Titolare del trattamento;
7. applicare ogni ulteriore limitazione e garanzie supplementari se anche solo occasionalmente il trattamento si estenderà a dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici o dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o dati relativi a condanne penali e a reati («dati sensibili»);
8. informare il Titolare qualora, a suo parere, un'istruzione violi il Regolamento UE o altre disposizioni relative alla protezione dei dati;
9. rispondere prontamente e adeguatamente alle richieste di informazioni del Titolare del trattamento relative al trattamento dei dati conformemente al presente atto, fornendo al Titolare a semplice richiesta e con le modalità indicate da quest'ultimo, tutti i dati e le informazioni oggetto dei trattamenti affidati al Responsabile, atteso che le valutazioni sulla legittimità del trattamento di tali dati, dell'eventuale comunicazione a terzi o diffusione degli stessi spettano al Titolare, congiuntamente ai relativi adempimenti, ivi comprese le informative ai propri dipendenti e agli altri interessati inerenti al trattamento dei dati;

10. trattare, se del caso, per conto del Titolare, con le modalità indicate da quest'ultimo, dati e informazioni necessari a effettuare comunicazioni a carattere informativo e promozionale nonché a svolgere indagini o ricerche di mercato, fermo restando che le valutazioni di legittimità sull'utilizzo dei dati ai fini delle predette comunicazioni nonché gli adempimenti previsti dalla normativa vigente in materia di protezione dei dati personali sono di competenza del Titolare;
11. cancellare e/o restituire, su scelta del Titolare, tutti i dati personali dopo che è terminata la prestazione dei servizi relativi a ciascun trattamento, fatto salvo il caso in cui si verifichino circostanze autonome che giustifichino la continuazione del trattamento dei dati da parte del Responsabile, con modalità limitate previamente concordate con il Titolare del trattamento;
12. assistere il Titolare come di seguito specificato:
    a) il Responsabile del trattamento notifica prontamente al Titolare del trattamento qualunque richiesta ricevuta dall'interessato; non risponde egli stesso alla richiesta, a meno che sia stato autorizzato in tal senso dal Titolare del trattamento;
    b) il Responsabile del trattamento assiste il titolare del trattamento nell'adempimento degli obblighi di rispondere alle richieste degli interessati per l'esercizio dei loro diritti, tenuto conto della natura del trattamento;
    c) nell'adempiere agli obblighi di cui alle lettere a) e b), il Responsabile del trattamento si attiene alle istruzioni del Titolare del trattamento;
    d) il Responsabile del trattamento assiste il titolare del trattamento anche nel garantire il rispetto dei seguenti obblighi, tenuto conto della natura del trattamento dei dati e delle informazioni a disposizione del responsabile del trattamento:
        1) l'obbligo di effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali («valutazione d'impatto sulla protezione dei dati») qualora un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
        2) l'obbligo, prima di procedere al trattamento, di consultare il Garante qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare del trattamento per attenuare il rischio;
        3) l'obbligo di garantire che i dati personali siano esatti e aggiornati, informando senza indugio il Titolare del trattamento qualora il Responsabile del trattamento venga a conoscenza del fatto che i dati personali che sta trattando sono inesatti o obsoleti;
        4) gli obblighi di cui all'articolo 32 regolamento (UE) 2016/679;
13. adottare in concreto le seguenti misure tecniche e organizzative specifiche che il Responsabile del trattamento deve prendere per essere in grado di fornire l'assistenza di cui al punto precedente al Titolare del trattamento: adottare un registro del trattamento telematico che effettua in automatico una prima valutazione del livello del rischio per i diritti e le libertà delle persone fisiche; attivare un servizio di consulenza;
14. cooperare, in caso di violazione dei dati personali, con il Titolare del trattamento e assisterlo nell'adempimento degli obblighi che incombono a quest'ultimo a norma degli articoli 33 e 34 del Regolamento, ove applicabile, tenuto conto della natura del trattamento e delle informazioni a disposizione del Responsabile del trattamento, secondo le seguenti modalità:
    - in caso di una violazione dei dati personali trattati dal Titolare del trattamento, il Responsabile del trattamento lo assiste:

a) nel notificare la violazione dei dati personali al Garante, senza ingiustificato ritardo dopo che il Titolare del trattamento ne è venuto a conoscenza, se del caso, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche;
b) nell'ottenere le seguenti informazioni che, in conformità all'articolo 33, paragrafo 3, del Regolamento devono essere indicate nella notifica del Titolare del trattamento e includere almeno:
   1) la natura dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
   2) le probabili conseguenze della violazione dei dati personali;
   3) le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali, se del caso anche per attenuarne i possibili effetti negativi;
   4) qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo;
c) nell'adempiere, in conformità all'articolo 34 del Regolamento all'obbligo di comunicare senza ingiustificato ritardo la violazione dei dati personali all'interessato, qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche;

- in caso di una violazione dei dati personali trattati dal Responsabile del trattamento, quest'ultimo ne dà notizia al Titolare del trattamento senza ingiustificato ritardo dopo esserne venuto a conoscenza, con notifica contenente almeno:
   a) una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati in questione);
   b) i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni sulla violazione dei dati personali;
   c) le probabili conseguenze della violazione dei dati personali e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione, anche per attenuarne i possibili effetti negativi.
   d) qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo;

15. fornire al Titolare, a semplice richiesta e secondo le modalità indicate da quest'ultimo, i dati e le informazioni necessarie per consentire allo stesso di svolgere una tempestiva difesa in eventuali procedure instaurate davanti al Garante o all'Autorità Giudiziaria e relative al trattamento dei dati personali;
16. compiere tempestivamente quanto necessario per conformarsi a richieste pervenute dal Garante o dall'Autorità Giudiziaria o, comunque, dalle Forze dell'Ordine;
17. mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dal Regolamento UE e il rispetto degli obblighi di cui all'atto di nomina, consentendo e contribuendo alle attività di revisione delle attività di trattamento,

a intervalli ragionevoli o se vi sono indicazioni di inosservanza; nel decidere in merito a un riesame o a un'attività di revisione, il Titolare del trattamento può tenere conto delle pertinenti certificazioni in possesso del Responsabile del trattamento; il Titolare del trattamento può scegliere di condurre l'attività di revisione autonomamente o incaricare un revisore indipendente; le attività di revisione possono comprendere anche ispezioni nei locali o nelle strutture fisiche del Responsabile del trattamento e, se del caso, sono effettuate con un preavviso ragionevole e minimo di ventiquattro ore; su richiesta, le parti mettono a disposizione della o delle autorità di controllo competenti le informazioni di cui alla presente clausola, compresi i risultati di eventuali attività di revisione; su richiesta, le parti mettono a disposizione del Garante le informazioni di cui alla presente clausola, compresi i risultati di eventuali attività di revisione;

18. conservare in maniera ordinata e diligente la documentazione inerente alle attività di trattamento e alla attività oggetto di incarico, rendendola accessibile al Titolare o ai soggetti da questi designati per eventuali ispezioni che si svolgeranno alle seguenti condizioni:
    - il Titolare dovrà dare un preavviso minimo di ventiquattro ore;
    - il preavviso non è dovuto in caso di violazioni di dati personali;
    - il Titolare potrà disporre un accesso presso la sede del Responsabile o altro luogo nella disponibilità giuridica del Responsabile in cui sia conservata la documentazione relativa alle attività di trattamento;
    - i costi della ispezione sono sostenuti dal Titolare;
    - i costi delle ispezioni saranno addebitati al Responsabile, qualora, all'esito delle stesse, risulti un grave inadempimento agli obblighi di cui al presente affidamento;
    - il Titolare deve dare preventiva comunicazione al Responsabile delle generalità dei soggetti incaricati delle verifiche;
    - in generale, prestare la più ampia e completa collaborazione al Titolare e al suo Responsabile per la Protezione dei Dati (Data Protection Officer), al fine di compiere tutto quanto sia necessario e opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente;
19. in generale, prestare la più ampia e completa collaborazione al Titolare e al suo Responsabile per la Protezione dei Dati (Data Protection Officer), al fine di compiere tutto quanto sia necessario e opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente.

Il Responsabile può subcontrattare a un sub-responsabile del trattamento i trattamenti da effettuare per conto del Titolare del trattamento conformemente alle clausole del presente atto, previa autorizzazione specifica scritta del Titolare del trattamento. Il Responsabile del trattamento presenta la richiesta di autorizzazione specifica almeno sette giorni prima di ricorrere al sub-responsabile del trattamento in questione, unitamente alle informazioni necessarie per consentire al Titolare del trattamento di decidere in merito all'autorizzazione. Il Titolare è tenuto a rispondere entro i successivi sette giorni, con applicazione dell'istituto del silenzio assenso. Il Titolare e il Responsabile tengono un elenco aggiornato dei sub-responsabili del trattamento autorizzati dal Titolare.

Quando il Responsabile ricorre a ulteriori eventuali Responsabili del Trattamento per specifiche attività di trattamento, deve trasferire su di essi le disposizioni del Titolare e adottare opportune

clausole contrattuali al fine di richiamare l'obbligo in capo ai medesimi di rispettare le misure di sicurezza descritte nell'atto di affidamento. Inoltre, l'atto che regola il rapporto del Responsabile con il sub-responsabile deve descrivere anche le misure tecniche e organizzative specifiche che il sub-responsabile del trattamento deve prendere per essere in grado di fornire assistenza al titolare del trattamento. Qualora il sub-responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, la società conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del sub-responsabile.

Su richiesta del Titolare del trattamento, il Responsabile del trattamento gli fornisce copia del contratto stipulato con il sub-responsabile del trattamento e di ogni successiva modifica. Nella misura necessaria a proteggere segreti aziendali o altre informazioni riservate, compresi i dati personali, il responsabile del trattamento può espungere informazioni dal contratto prima di trasmetterne una copia.

Il Responsabile del trattamento rimane pienamente responsabile nei confronti del Titolare del trattamento dell'adempimento degli obblighi del sub-responsabile del trattamento derivanti dal contratto che questi ha stipulato con il responsabile del trattamento. Il Responsabile del trattamento notifica al titolare del trattamento qualunque inadempimento, da parte del sub-responsabile del trattamento, degli obblighi contrattuali.

Il Responsabile del trattamento concorda con il sub-responsabile del trattamento una clausola del terzo beneficiario secondo la quale, qualora il Responsabile del trattamento sia scomparso di fatto, abbia giuridicamente cessato di esistere o sia divenuto insolvente, il titolare del trattamento ha diritto di risolvere il contratto con il sub-responsabile del trattamento e di imporre a quest'ultimo di cancellare o restituire i dati personali.

Qualunque trasferimento di dati verso un paese terzo o un'organizzazione internazionale da parte del Responsabile del trattamento o del sub-responsabile è effettuato soltanto su istruzione documentata del Titolare del trattamento o per adempiere a un dovere giuridico derivante dal diritto nazionale o europeo, e nel rispetto del capo V del regolamento (UE) 2016/679.

Fatte salve le disposizioni del regolamento (UE) 2016/679, qualora il Responsabile del trattamento violi gli obblighi che gli incombono a norma del presente atto, il Titolare del trattamento può dare istruzione al Responsabile del trattamento di sospendere il trattamento dei dati personali fino a quando quest'ultimo non rispetti le relative clausole o non sia risolto il rapporto. Il Responsabile del trattamento informa prontamente il Titolare del trattamento qualora, per qualunque motivo, non sia in grado di rispettare il presente atto.

Il Titolare del trattamento ha diritto di revocare l'incarico per quanto riguarda il trattamento dei dati personali a norma del presente atto qualora:

1) il trattamento dei dati personali da parte del Responsabile del trattamento sia stato sospeso dal Titolare del trattamento nei casi consentiti e il rispetto delle clausole dell'atto non sia ripristinato entro un termine ragionevole e in ogni caso entro un mese dalla sospensione;
2) il Responsabile del trattamento violi in modo sostanziale o persistente le clausole del presente atto o gli obblighi che gli incombono a norma del Regolamento (UE) 2016/679;

3) il Responsabile del trattamento non rispetti una decisione vincolante di un organo giurisdizionale competente o del Garante per quanto riguarda i suoi obblighi in conformità delle clausole del presente atto o del Regolamento (UE).

Il Responsabile del trattamento ha diritto di recedere dall'incarico per quanto riguarda il trattamento dei dati personali a norma del presente atto qualora, dopo aver informato il titolare del Trattamento che le sue istruzioni violano il Regolamento, il titolare del trattamento insista sul rispetto delle istruzioni.

Dopo la revoca o il recesso il Responsabile del trattamento, a scelta del Titolare del trattamento, cancella tutti i dati personali trattati per conto del titolare del trattamento e certifica a quest'ultimo di averlo fatto, oppure restituisce al Titolare del trattamento tutti i dati personali e cancella le copie esistenti, salvo diversa disposizione di diritto interno o europeo che richieda la conservazione dei dati personali. Finché i dati non sono cancellati o restituiti, il Responsabile del trattamento continua ad assicurare il rispetto delle presenti clausole

L'atto di incarico deve infine recare la precisazione che: - quando l'atto stesso utilizza termini definiti dal Regolamento (UE) 2016/679, tali termini hanno lo stesso significato di cui al menzionato Regolamento; l'intero contenuto dell'atto deve essere letto e interpretato alla luce delle disposizioni del Regolamento (UE) 2016/679 e non deve essere interpretato in un senso che non sia conforme ai diritti e agli obblighi previsti dallo stesso o che pregiudichi i diritti o le libertà fondamentali degli interessati; in caso di contraddizione tra il contenuto dell'atto e le clausole di cui alla Decisione della Commissione Europea 2021/915, prevalgono queste ultime.

Ogni specifico atto di incarico potrà prevedere prescrizioni aggiuntive in relazione alla specificità del trattamento effettuato dal Responsabile per conto della Azienda.
Qualora si rendesse necessario derogare o modificare tali prescrizioni, l'atto di incarico deve contenere apposita motivazione e puntuale giustificazione.

FORNITORI – CONSULENTI – COLLABORATORI – INCARICATI A QUALSIASI TITOLO

Ai fornitori, consulenti, collaboratori e a qualsiasi altro soggetto incaricato dall'Azienda a svolgere a suo favore una determinata prestazione che implica la possibilità anche occasionale di venire a conoscenza dei dati personali posti nella titolarità dell'ente, devono essere impartite, mediante idonee clausole contrattuali, le opportune istruzioni, con attribuzione della relativa responsabilità in riferimento agli eventuali trattamenti oggetto dell'incarico stesso.

FORMAZIONE ED INFORMAZIONE INTERNA

Nell'ottica di diffondere le conoscenze relative alla materia e di fornire adeguate istruzioni a tutto il personale aziendale:

- tutta la documentazione relativa al Sistema di Gestione della Privacy è resa disponibile mediante condivisione in apposita cartella della intranet ovvero con forme equivalenti;
- il funzionamento del Sistema di Gestione è presentato e descritto a tutto il personale in specifici incontri di condivisione, al fine di agevolarne la conoscenza e lo svolgimento dei ruoli e delle attività previste;
- sono realizzati progetti formativi specifici:
  - per i dipendenti che coadiuvano il Delegato per gli adempimenti di propria competenza;
  - per i dipendenti eventualmente incaricati di svolgere la funzione di amministratore di sistema;
- potranno inoltre essere pianificati ulteriori specifici percorsi o eventi secondo le modalità ritenute più idonee (seminari, workshop, convention, incontri frontali e altri), nei quali si terrà conto anche delle specifiche esigenze comunicate dal personale.

L'organizzazione di tali percorsi ed eventuali specifiche azioni formative

✓ saranno progettati e gestiti operativamente dal Titolare;
✓ saranno monitorate sia per quanto riguarda la realizzazione che gli esiti dal RPD.

Il personale potrà inoltre fare riferimento direttamente al RPD (attraverso la specifica casella di posta elettronica) per la proposta di quesiti, la richiesta di approfondimenti, anche previa condivisione con la sua struttura di supporto. E' sempre diretta la possibilità di contattare il RPD qualora la questione proposta attenga alla tutela dei propri dati personali.

Ulteriori attività di formazione/informazione saranno programmate al momento dell'assunzione di nuove risorse, nonché in occasione di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti rilevanti rispetto al trattamento di dati personali.

STRUMENTI PER IL MONITORAGGIO E CONTROLLO DEL SISTEMA

REGISTRAZIONI, DOCUMENTAZIONE E FLUSSI INFORMATIVI

L'attuazione di un sistema di **monitoraggio, verifica e controllo** del sistema privacy implementato rispetto alla normativa e alle direttive e istruzioni impartite è una specifica

responsabilità del Titolare del trattamento, rientrante negli obblighi di accountability di cui agli artt. 24[1] e 32[2] del GDPR.

Il sistema di monitoraggio, verifica e controllo poggia su due livelli distinti di intervento:

- ❖ controllo di primo livello (c.d. "controllo di linea"), posto in essere dal Delegato coadiuvato dai soggetti "Autorizzati Responsabili" nell'ambito delle ordinarie funzioni di coordinamento e gestione delle attività di propria competenza;
- ❖ controllo di secondo livello (c.d. "controllo di compliance") affidato al RPD come descritto nell'apposito paragrafo del presente documento.

Gli specifici strumenti messi a disposizione di tali soggetti sono i seguenti:

a) **Registro dei Data Breach**: il registro consente la registrazione e tracciamento degli eventi (anche non sfociati in un incidente), degli incidenti e quasi-incidenti (situazioni anomale o incidenti di sicurezza) nonché dei veri e propri data breach, a prescindere se l'evento abbia dato luogo alla notifica al Garante e/o alla comunicazione agli interessati di cui agli artt. 33 e 34. Così configurato, il Registro consente di identificare e circoscrivere (per "tipologia di eventi" ovvero per asset/trattamento) gli ambiti di criticità maggiormente impattanti - in termini organizzativi, operativi e di compliance - sull'organizzazione ed eventualmente sugli interessati, al fine di poter evidenziare i principali o più critici ambiti di intervento da gestire mediante azioni correttive;

b) **Registro delle richieste di esercizio dei diritti degli interessati**: anche in questo caso, oltre a costituire un fondamentale strumento documentale per tracciare e poter dimostrare la compliance sul punto, il Registro consente di individuare eventuali attività o modalità di trattamento considerate "critiche" dagli interessati.

La tenuta dei Registri, appositamente approvati dal Titolare, è affidata al RPD e gestita dalla sua struttura di supporto, mentre l'alimentazione degli stessi è garantita dai flussi informativi appresso regolati.

Ulteriori documenti e dati di input ai fini del monitoraggio e controllo del sistema privacy possono essere i seguenti:

- ✓ rendicontazioni periodiche e/o finali dei progetti/servizi affidati all'esterno, mediante specifica previsione contrattuale in capo al Responsabile esterno ex art. 28 del GDPR di relazionare sul buon esito delle attività di trattamento secondo le istruzioni impartite;
- ✓ relazioni periodiche circa l'andamento delle attività di competenza degli amministratori di sistema;

[1] "… il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario".

[2] "… il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso… d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento".

- ✓ audit report e relazioni periodiche formalizzate dal RPD nel corso degli audit e verifiche di competenza;
- ✓ rilevazione dei dati e valorizzazione degli indicatori di anomalia di cui al paragrafo seguente e conseguente verifica dello scostamento rispetto ai valori obiettivo ivi definiti (da considerarsi quali "alert" ovvero indici di situazioni di rischio potenziale).

Per effetto dell'approvazione del presente documento sono istituiti i seguenti **flussi informativi in favore del RPD**:

PERIODICITÀ	DESCRIZIONE FLUSSO INFORMATIVO	RESPONSABILE FLUSSO
Tempestiva	Copia delle richieste di informazioni da parte di organi di Polizia Giudiziaria (ad es., Carabinieri, Polizia, Guardia di Finanza, etc.) o dal Garante e di tutti i verbali di accesso e di contestazione a seguito di ispezioni e controlli	Delegato Referente Privacy
Tempestiva	Sanzioni comminate da Pubbliche autorità in materia di privacy	Delegato Referente Privacy
Tempestiva	Copia relazioni / verbali redatti in sede di audit di I livello in cui si evidenzino criticità lato privacy	Delegato Referente Privacy
Quadrimestrale	Schede di rilevazione eventi (cfr. procedura data breach)	Delegato Referente Privacy
Quadrimestrale	Verbali di analisi degli incidenti (cfr. procedura di data breach)	Delegato Referente Privacy
Quadrimestrale	Risposte agli interessati in caso di reclami/esercizio diritti	Delegato Referente Privacy
Tempestiva	Informativa relativa al rifiuto di assunzione del ruolo/designazione a Responsabile esterno del trattamento	Delegato Referente Privacy

INDICATORI DI ANOMALIA DEL SISTEMA PRIVACY

Il seguente sistema di indicatori è gestito dal RPD ed è alimentato mediante gli strumenti di registrazione ed i flussi di cui al par. precedente.

DIMENSIONE DEL MONITORAGGIO	DESCRIZIONE INDICATORE	VALORE SEGNALETICO	FONTE DI REPERIMENTO DEL DATO
COMPLIANCE ALLA NORMATIVA	Numero di richieste di esercizio dei diritti ex artt. 15 e ss. del GDPR o di reclami pervenuti dagli interessati nell'anno	> 5	Registro delle richieste di esercizio dei diritti
	Numero di richieste/reclami con identico oggetto o relative ad uno stesso trattamento	> 3	
	Tempi di risposta alle richieste di esercizio dei diritti da parte degli interessati	≤ 30 gg	
	Numero di ispezioni subite da pubbliche autorità su segnalazione/denuncia degli interessati nell'anno	> 1	Flussi informativi al RPD
	Numero di sanzioni comminate in materia da pubbliche autorità nell'anno	> 0	
	Numero di soggetti esterni che hanno rifiutato la designazione a Responsabile esterno del trattamento	> 2	
CONTROLLO E MIGLIORAMENTO CONTINUO	Numero di privacy audit effettuati nell'anno	≤ 1	Verbali/relazioni di audit/ Relazioni agli Organi
	% di Non Conformità (NC) riscontrate (n. NC / n. audit)	≥ 20%	
	Numero relazioni del RPD agli Organi	< 1	Relazioni agli Organi
SICUREZZA E DISPONIBILITÀ DEI DATI	Numero di segnalazioni di incidenti inserite nel Registro dei Data Breach	≥ 3/anno	Registro data breach
	Numero di violazioni di dati personali notificate al Garante Privacy ex art. 33 GDPR	> 1	
	Numero di data breach notificati al Garante oltre i termini previsti dal GDPR (72h)	> 1	
	Numero di violazioni di dati personali comunicate agli interessati ex art. 34 GDPR	> 1	

	Tempi medi di risoluzione incidenti e problematiche di sicurezza (sommatoria giorni tra segnalazione e risoluzione / numero segnalazioni)	≥ 7	Sistema ticketing interno / fornitori esterni
	Tempi medi di risoluzione incidenti bloccanti (sommatoria giorni tra segnalazione e risoluzione / numero segnalazioni)	≥ 2	

PRIVACY AUDIT

La realizzazione di verifiche e audit al fine di verificare l'applicazione della normativa e delle istruzioni impartite è funzione affidata - nelle fasi di rilevazione dell'esigenza, programmazione e realizzazione – al RPD coadiuvato dalla struttura di supporto.

Le attività di verifica sono di regola programmate e previamente comunicate ai soggetti coinvolti (salvo esigenze di audit a sorpresa) e sempre condotte alla presenza degli stessi.

Gli esiti delle verifiche, formalizzati in forma di audit report, sono:

- condivise con i soggetti auditi che possono formalizzare chiarimenti e/o controdeduzioni,
- completate – in caso di rilevazione di Non conformità (NC) – dalla proposta di azioni correttive/preventive,
- formalizzate – immediatamente ove evidenzino NC, ovvero nell'ambito delle relazioni periodiche – al Consiglio.

A seguito della conduzione degli audit, il RPD provvede ad alimentare gli indicatori di cui al paragrafo precedente.

RIESAME E AGGIORNAMENTO DEL SISTEMA DI GESTIONE DELLA PRIVACY

Nell'ottica del miglioramento continuo e del raggiungimento degli obiettivi di compliance alla normativa di riferimento, anche al fine di garantire che l'efficacia delle misure tecniche e organizzative implementate sia "testata regolarmente" (art. 32, par. 1, lett. d), del GDPR), il Sistema di gestione della Privacy delineato nel presente documento dovrà essere sottoposto a riesame, in occasione:

- dell'emanazione di nuove disposizioni normative, di pronunce giurisprudenziali, ovvero in relazione ad eventuali provvedimenti del Garante per la Protezione dei Dati di carattere cogente e/o interpretativo che abbiano un impatto sulla disciplina della protezione dei dati rilevante per l'Ente;
- di cambiamenti significativi della struttura organizzativa o dei settori di attività dell'Ente che comportino la ridefinizione della governance interna, degli organigrammi e delle relative attività e responsabilità;
- in occasione dell'introduzione di nuovi significativi strumenti di gestione, rilevanti rispetto al trattamento di dati personali;

- nel caso di applicazione di sanzioni da parte dell'Autorità giudiziaria ovvero del Garante nella materia di cui trattasi.

Il riesame è istruito con la collaborazione del RPD, il quale redigerà, ove richiesto, apposita relazione in merito, tenuto conto delle informazioni disponibili quali desunte dalle proprie attività di supporto e di controllo. L'eventuale relazione del RPD è trasmessa al CDA per l'assunzione delle eventuali decisioni necessarie a garantire la compliance e il miglioramento continuo.