MODELLO ORGANIZZATIVO PRIVACY (MOP)
POLICY PRIVACY

Ruoli e sistema di responsabilità, ai sensi del Regolamento UE

2016/679, articolo 24

Approvato dal Consiglio di Amministrazione in data 29 maggio 2024

PREMESSA

PRIVACY

Il 25 maggio 2018 è divenuto pienamente e direttamente applicabile in tutti gli Stati membri dell'Unione europea il Regolamento 2016/679, così detto **GDPR** (*GENERAL DATA PROTECTION REGULATION*), "*relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*", il quale ha tra i suoi obiettivi e novità quelli di:

- armonizzare la disciplina sulla protezione dei dati personali all'interno di tutta l'Unione europea;
- rafforzare e introdurre nuovi diritti degli interessati;
- attribuire fondamentale importanza ai principi della: a) *accountability*, b) *privacy by design*, c) *by default*,
- inasprire le sanzioni portandole sino a € 20.000.000 o al 4% del fatturato mondiale annuo del gruppo;
- introdurre la figura del *DATA PROTECTION OFFICER* (*DPO*).

La struttura del GDPR è articolata: consta di 99 articoli, racchiusi in 11 capi, preceduti da 173 "*considerando*". Con l'entrata in vigore del GDPR è stata abrogata la c.d. "*direttiva madre*" sul trattamento dei dati (la direttiva 95/46/CE) e il legislatore comunitario ha inteso assicurare l'uniformità normativa e l'omogeneità applicativa all'interno dell'Unione europea al fine favorire la circolazione dei dati e la creazione (si veda il settimo "*considerando*") di un «*clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno*».

Principio ispiratore della normativa comunitaria è quello di *accountability* ("*responsabilizzazione*" e/o "*rendicontazione*") che onera il titolare del trattamento a mettere «*in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al [...] regolamento*» (articolo 24, paragrafo 1).

Alla legislazione europea continua ad affiancarsi quella nazionale e, in particolare:

- il "*Codice in materia di dati personali*" o "*Codice della privacy*", contenuto nel Decreto Legislativo 30 giugno 2003 n. 196, come modificato dal Decreto Legislativo 10 agosto 2018 n. 101 "*Codice in materia di protezione dei dati personali*" (Codice della Privacy), come modificato dal D.lgs. 10 agosto 2018, n. 101 (in seguito **Codice**), recante disposizioni di adeguamento della disciplina italiana ai dettami del GDPR
- e i provvedimenti emanati nel tempo dal Garante Europeo della Protezione dei Dati (GEPD) e dall'Autorità Garante Nazionale per la protezione dei dati personali (in seguito **Garante**).

SCOPO E DEFINIZIONI

L'**AZIENDA DI PROMOZIONE E SVILUPPO TURISTICO DI LIVIGNO S.R.L.** (in seguito **APT**) intende dotarsi di linee guida che consentano di affrontare in maniera organica gli obblighi normativi in materia di protezione dei dati personali, così da conseguire i migliori risultati nel proteggere le informazioni e i dati gestiti nell'ambito delle proprie attività da tutte le minacce interne o esterne, intenzionali o accidentali, secondo le disposizioni previste dalla normativa comunitaria e nazionale

Obiettivo del presente documento - e di quelli ad esso collegati - è definire il ***MODELLO ORGANIZZATIVO PRIVACY*** (MOP), ovvero individuare strategia, linee guida generali e disposizioni operative interne volte a disciplinare il trattamento dei dati personali effettuato dall'APT, ai sensi del Codice e del GDPR nonché ulteriori provvedimenti in materia di fonte normativa secondaria in vigore al momento dell'approvazione della seguente *policy*.
In essa sono, quindi, disciplinati i ruoli e le responsabilità nonché gli adempimenti da seguire in materia di protezione dei Dati Personali ai sensi del Codice e del GDPR, anche con riferimento alle decisioni e ai provvedimenti emessi dal Garante.
Ai fini del presente Modello Organizzativo Privacy si applicano le seguenti definizioni, coerenti con quanto previsto dalla normativa di settore:

- Regolamento: Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE (GDPR - Regolamento Generale sulla Protezione dei Dati);
- Normativa: D.lgs. 2003/196 (come modificato dal D.lgs. 2018/101) e Regolamento (UE) 2016/679, nonché ulteriori provvedimenti in materia di fonte normativa secondaria in vigore al momento dell'approvazione del presente Modello Organizzativo Privacy;
- Codice Privacy: Decreto legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" come modificato dal Decreto Legislativo 10 agosto 2018, n. 101;
- Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («*interessato*»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- Dati genetici: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- Dati biometrici: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- Dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- Interessato: la persona fisica cui si riferiscono i dati personali;
- Titolare del trattamento: è l'APT che determina le finalità e i mezzi del trattamento di dati personali e che tramite il legale rappresentante effettua la sorveglianza sull'applicazione e il rispetto delle disposizioni in materia di trattamento di dati, al quale sono affidati anche compiti di coordinamento di più o soggetti autorizzati (o *designati)*;
- Responsabile del trattamento: la persona fisica che tratta dati personali per conto del titolare del trattamento;
- Autorizzato: le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare del trattamento o dal Responsabile del trattamento (anche soggetti *designati*);
- 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 del trattamento o del responsabile del trattamento;
- 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;

- Paesi terzi: paesi non appartenenti all'UE o allo spazio Economico Europeo (Norvegia, Islanda, Liechtenstein);

CAMPO DI APPLICAZIONE

Il principio *PRIVACY BY DESIGN*, previsto dall'articolo 25 dal GDPR, ha lo scopo di garantire l'esistenza di un corretto livello di *privacy* e protezione dei dati personali fin dalla fase di progettazione (*design*) di qualunque sistema, servizio, prodotto o processo così come durante il loro ciclo di vita: quindi garantire un corretto livello di protezione dei dati in tutte le attività di trattamento ed attuazioni effettuate all'interno di una organizzazione. Conseguentemente, si rende necessario valutare e predisporre le misure tecniche ed organizzative nel rispetto i principi fondamentali della protezione di dati specificati nell'articolo 5 del GDPR, quali trasparenza, limitazione delle finalità e minimizzazione. In particolare, il trattamento dei dati personali deve essere effettuato nel rispetto del "*criterio di minimizzazione*", in virtù del quale essi devono essere utilizzati solo se indispensabili, pertinenti e limitati a quanto necessario per il perseguimento delle finalità per cui sono raccolti e trattati (ad esempio, come precisato dalla giurisprudenza, ne consegue che la fedele trascrizione, in un articolo, del contenuto di un'informativa di reato della polizia giudiziaria non esime l'autore dall'obbligo di depurarla dei dati personali la cui conoscenza sia del tutto ininfluente in relazione al contenuto informativo dell'articolo stesso).
A ciò si aggiunga che In tema di illecito trattamento dei dati personali reputazionali, in base alla disciplina generale del GDPR, il titolare del trattamento dei dati personali è sempre tenuto a risarcire il danno cagionato a una persona da un trattamento non conforme al regolamento stesso e può essere esonerato dalla responsabilità non semplicemente se si è attivato (come suo dovere) per rimuovere il dato illecitamente esposto, ma solo se dimostra che l'evento dannoso non gli è in alcun modo imputabile. (Nella specie, la S.C. ha confermato la sentenza di merito che aveva ravvisato la violazione del GDPR nella condotta del Comune che aveva pubblicato nell'albo pretorio on line, sia pure per un giorno, la nota contabile contenente i dati della dipendente destinataria del pignoramento del proprio stipendio e rispetto alla quale l'ente aveva assunto l'impegno di versarne il quinto alla società creditrice, non essendo all'uopo rilevante la riconducibilità del fatto a errore umano ed essendo l'ente responsabile anche del fatto colposo dei suoi dipendenti).
Dall'articolo 25 del GDPR si evince, inoltre, che l'approccio del Regolamento UE sia centrato, tra l'altro, sulla valutazione del rischio (*RISK BASED APPROACH*), per cui le aziende devono valutare il rischio inerente alle loro attività.
Con tale valutazione si determina la misura di responsabilità del titolare o del responsabile del trattamento, tenendo conto della natura, della portata, del contesto e delle finalità del trattamento, nonché della probabilità e della gravità dei rischi per i diritti e le libertà degli utenti. Tale valutazione del rischio va fatta al momento della progettazione del sistema, quindi prima che il trattamento inizi.
Scopo del presente documento è quello di assicurare la *compliance* ("*conformità*") al GDPR e al Codice mediante un processo permanente di adeguamento, al fine di definire il modello organizzativo per la gestione degli adempimenti in materia di protezione dei dati e degli interessati, emanati nel tempo dal Garante per la protezione dei dati personali. In particolare, il documento regolamenta:

a) i ruoli e le responsabilità assegnate;
b) la modulistica per la gestione del 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 utilizzando il processo di formazione attuato con il Piano Triennale Anticorruzione Integrato con il modello 231.

PROCESSO DI ADEGUAMENTO

Per adeguarsi alla normativa privacy è necessario seguire i seguenti **passaggi iniziali**:

1. **Creare una *privacy policy***: per informare le persone sulle finalità e sulle modalità di trattamento dei loro dati personali.
2. **Gestire i *cookie***: per informare gli utenti di un sito o di una *app* su quali *cookie* vengono memorizzati.
3. **Creare un registro dei trattamenti**: ove previsto, per tracciare la raccolta dei dati personali di clienti, collaboratori, fornitori e *partner.*
4. **Nominare un responsabile del trattamento**: per incaricare un soggetto all'attività per trattare i dati per conto del titolare.
5. **Verificare gli altri adempimenti**: per rispettare ogni altro obbligo sulla *privacy* (es. fare una valutazione di impatto)

1. Creare una *privacy policy*

La *privacy policy* sul trattamento dei dati (Informativa *Privacy*) è il documento di partenza per essere a norma. Questa policy **informa le persone** sulle finalità e sulle modalità di trattamento dei loro dati. Il dato personale è ogni informazione che identifica una persona direttamente o indirettamente (es. il nome e il cognome o il codice fiscale). L'informativa va creata ogni volta in cui si effettua un trattamento dei dati. Vale a dire qualunque operazione effettuata (es. raccolta, cancellazione e invio a terzi dei dati personali). Bisogna creare l'informativa anche quando il **dato è trattato *online***. Ad esempio, quando vengono raccolti l'indirizzo *IP*, le pagine visitate e le coordinate GPS di un utente sul *web*. In questi casi, si parla di *privacy policy* di un sito *web* o di un *app*.

2. Gestire i *cookie*

Quando il trattamento dei dati avviene *online*, vengono spesso usati dei *cookie*. Si tratta di **file di navigazione** che vengono memorizzati sul dispositivo di un utente che visita un sito. I cookie salvano i dati di navigazione dell'utente e possono essere usati per diversi scopi. Ad esempio, il titolare di un sito può usare i *cookie* per tracciare il comportamento dell'utente a fini statistici. Se si usano i cookie, è **necessario informare gli utenti** su quali dati vengono memorizzati. Inoltre, occorre ottenere il consenso dell'utente prima dell'installazione dei *cookie*. In particolare, bisogna:

a. creare un'**informativa estesa** (*cookie policy*). Si tratta di una pagina che specifica le categorie di *cookie* utilizzati e le finalità;

b. creare un'**informativa breve** (o *cookie banner*). Si tratta di un avviso dinamico che consente agli utenti di gestire il consenso all'installazione attraverso dei pulsanti dedicati (es. "*Accetto tutti i cookie*" o "*Rifiuto tutti i cookie*")

3. Creare un registro dei trattamenti, ove previsto in ragione dell'organico.

Uno dei più importanti adempimenti *privacy* è la creazione di un registro dei trattamenti dei dati personali. È stato **introdotto con il regolamento europeo** sulla *privacy* (GDPR). Questo registro si usa per conservare le informazioni sulle operazioni effettuate sui dati.

Il registro non è sempre obbligatorio, tuttavia, è **ritenuto opportuno** per:

- conservare e **mappare le informazioni** principali sul trattamento dei dati (es. tipi di dati, finalità del trattamento e tempo di conservazione)
- **tenere traccia della propria conformità** alla normativa *privacy* e avere una prova scritta da poter mostrare in caso di richiesta da parte delle autorità competenti

4. Nominare un responsabile del trattamento

La nomina del responsabile di trattamento è un adempimento previsto quando si deve autorizzare un **soggetto esterno a trattare i dati** personali per conto del titolare. In questi casi, il titolare decide quali dati personali raccogliere e per quale motivo. Il responsabile, invece, effettua le operazioni sui dati in base alle istruzioni del titolare. L'esempio tipico è il consulente del lavoro che si occupa delle buste paga e delle assunzioni dei collaboratori del titolare.

5. Verificare gli altri adempimenti privacy

Gli adempimenti privacy appena descritti sono solo alcuni dei passaggi previsti dalla legge. Infatti, in base alle caratteristiche e alle modalità di trattamento dei dati si applicano regole diverse. Vediamo alcuni esempi concreti di **altri adempimenti**:

- adozione di misure di sicurezza: pratiche tecniche o organizzative previste per garantire la sicurezza dei dati personali (es. la cifratura dei dati)
- effettuare una valutazione di impatto: un'attività di analisi per identificare potenziali rischi connessi a delicate operazioni compiute sui dati personali (es. monitoraggio sistematico in videosorveglianza su larga scala)
- nomina di un *DATA PROTECTION OFFICER* (*DPO*): il responsabile della protezione dei dati personali supporta e controlla l'applicazione della normativa privacy e deve essere nominato in alcuni casi particolari (es. in caso di trattamento di dati sensibili su larga scala)

Al fine di assicurare la compliance ("*conformità*") l'**APT** ha intrapreso un processo permanente di adeguamento. E così, in linea di coerenza con il principio di *accountability*:

A) si è provveduto:

1) alla designazione del responsabile della protezione dei dati (RPD) (articolo 37 del GDPR), con delibera del Consiglio di Amministrazione;

2) alla definizione di una procedura interna per l'adeguata e tempestiva gestione degli incidenti di sicurezza "*c.d. data BREACH*" (articoli 33 e 34 del GDPR) e alla istituzione di un "*registro delle violazioni dei dati personali*";

3) alla redazione delle informative (articoli 13 e 14 del GDPR) e precisamente:

- informativa sul trattamento dei dati personali dei dipendenti e collaboratori;
- informativa sulla videosorveglianza;
- informativa sul trattamento dei dati personali degli utenti del portale *web*;
- informativa sul trattamento dei dati personali di operatori economici, fornitori e collaboratori esterni;
- informativa sul trattamento dei dati personali per le riprese fotografiche e televisive, registrazioni audio, videoregistrazioni;

4) alla costituzione di un gruppo di lavoro di supporto al titolare del trattamento e al responsabile della protezione dei dati.

Non si è provveduto all'adozione del registro delle attività di trattamento (articolo 30 del GDPR), tenuto conto che tale obbligo non si applica alle imprese con meno di 250 dipendenti e il trattamento che viene effettuato non presenta "*un rischio per i diritti e le libertà dell'interessato*"

B) A programmare i seguenti interventi, ritenuti essenziali nel processo di adeguamento:

- definizione piano di formazione/azione per i responsabili di posizione organizzativa;
- organizzazione di eventi formativi e di corsi (anche *on line*) volti a favorire la massima diffusione della cultura della *privacy* tra tutti i dipendenti e i collaboratori;
- nomina a responsabili del trattamento dei principali fornitori di servizi che trattano dati personali per conto dell'APT;
- aggiornamento della cartellonistica sulla videosorveglianza, con i nuovi riferimenti normativi, nei vari locali ove si svolge l'attività dell'APT;
- formalizzazione di un archivio contenente gli interventi preventivi di sicurezza informatica;
- abilitazione del personale preposto della gestione delle pratiche dei dipendenti personale

per i documenti trattanti dati personali delicati, nello specifico in ambito di salute;

- aggiornamento della modulistica relativa all'ambito salute del personale tecnico amministrativo: la modulistica è stata ridisegnata minimizzando le informazioni richieste *ex ante* e valorizzando le uniche informazioni necessarie alla corretta esecuzione del procedimento amministrativo.

C) Si provvederà con cadenza annuale:

- alla continua sollecitazione tra i dipendenti degli uffici amministrativi della sensibilità sul rispetto della normativa;

- alla individuazione e implementazione di misure di *privacy by default* e *by design* (articolo 25 del GDPR);
- alla valutazione d'impatto (DPIA articolo 35 del GDPR) dei trattamenti che presentano un rischio elevato per i diritti e per le libertà delle persone fisiche;
- alla continua verifica della posizione dei fornitori di beni e servizi dell'APT ai fini della loro eventuale nomina a responsabili (esterni) del trattamento (articolo 28 del GDPR);
- allo svolgimento di interviste al personale impiegato negli uffici dell'APT da parte di alcuni componenti del gruppo di supporto al titolare del trattamento e al responsabile della protezione dei dati (RPD), finalizzate all'integrazione e all'aggiornamento del registro dei trattamenti;
- all'aggiornamento di tutta la modulistica di APT con i nuovi riferimenti normativi;
- alla valutazione in merito alla creazione di figure di delega sui vari trattamenti opportunamente formate;
- all'attivazione piano di formazione/azione per i responsabili di posizione organizzativa e formazione personale.

LA GESTIONE DELLA SICUREZZA: RUOLI E RESPONSABILITA'

RIFERIMENTI NORMATIVI

1. Titolare del trattamento (articolo 4, n. 7 e articolo 24 del GDPR);
2. Responsabile della Protezione dei Dati (articoli 37, 38 e 39. del GDPR);
3. Soggetti che trattano dati "*per conto"* e sotto l'autorità del Titolare del trattamento (articolo 29 del GDPR);
4. Attribuzione di funzioni e compiti a soggetti designati (articolo 2-quaterdecies del Codice);
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 successive modificazioni ed integrazioni.

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 dalla Società con riguardo alle potestà decisionali. In linea con tale interpretazione e sulla base della lettura delle competenze istituzionali degli organi di vertice dell'APT e ferma restando la qualifica di Titolare del trattamento da identificarsi nella struttura nel suo complesso e, quindi, in capo all'APT, le funzioni di natura gestionale che la legge attribuisce al Titolare, non possono che essere originariamente individuate in capo al Presidente del Consiglio di Amministrazione (in appresso **Presidente**) che, a mente dello Statuto, è l'organo amministrativo di gestione, sulla base dell'indirizzo politico definito dal Consiglio di Amministrazione (in appresso **Consiglio**) e, in ragione del rapporto *in house,* dal socio pubblico totalitario.
In tal senso, si ritiene che:
a) il Consiglio debba verificare la conformità del presente documento alla volontà politica, anche con riferimento alle indicazioni del socio pubblico;
b) il Presidente 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 GDPR e ai principi di:

- *accountability* (affidabilità e responsabilizzazione)
- e di *privacy by design & by default* (adozione di misure tecniche e organizzative adeguate alla protezione - trattamento dati per impostazione predefinita).

In considerazione di tali funzioni, Il Presidente provvede:

a) a nominare il Responsabile della Protezione dei Dati (RPD/DPO);

b) ad approvare i documenti gestionali per il regolare ed efficiente funzionamento del sistema privacy;

c) 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'APT al GDPR.

Conformemente a quanto previsto dalla normativa l'ente è Titolare del trattamento e in tale ruolo si impegna a:

- adeguare il proprio assetto organizzativo per rendere il governo della privacy allineato ai dettami normativi;
- adottare le modalità operative necessarie alla corretta gestione degli adempimenti ai fini della protezione dei dati personali trattati;
- assumere le decisioni in ordine alle finalità, alle modalità del trattamento dei dati e agli strumenti utilizzati, ivi compreso il profilo della sicurezza, sia per i trattamenti svolti all'interno che all'esterno della propria struttura;
- individuare e designare i Responsabili del trattamento dei dati, impartendo loro le relative direttive e, se necessario, istruzioni specifiche;
- vigilare sulla puntuale osservanza delle disposizioni e istruzioni impartite a tutti i soggetti che hanno un ruolo attivo nel trattamento dei dati personali;
- garantire sempre il pieno controllo sulla piramide organizzativa di cui è al vertice, concedendo autorizzazioni generali o specifiche ai responsabili del trattamento secondo criteri di opportunità nelle diverse situazioni ed esprimendo o negando il gradimento nei confronti di sub-responsabili eventualmente proposti dai responsabili assumendo così un ruolo di effettivo controllo e indirizzo.

Inoltre, si impegna a garantire l'esercizio dei diritti degli interessati e a tal scopo individua e mette in pratica apposite procedure al fine di informare gli interessati e garantire a ciascuno di essi almeno il:

a) diritto all'accesso, cioè di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano e di averne accesso. In particolare, l'interessato ha diritto di conoscere l'origine dei dati personali; le finalità e modalità del trattamento; la logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; gli estremi identificativi del titolare, dei responsabili e degli eventuali rappresentanti designati; l'elenco dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza a qualsiasi titolo in linea con la normativa e quello dei soggetti autorizzati al trattamento;

b) diritto alla rettifica, cioè di ottenere l'aggiornamento, la correzione ovvero, quando vi ha interesse, l'integrazione dei dati;

diritto alla cancellazione, cioè di ottenere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;

c) diritto all'opposizione, cioè di limitare od opporsi, per motivi legittimi, al trattamento, seguendo le modalità descritte dalle norme vigenti.

Al fine di esercitare i diritti sopra descritti, l'APT si impegna a rispondere senza ritardo alle richieste presentate da parte dell'interessato direttamente ad esso, ai Responsabili o ai soggetti autorizzati appositamente nominati, nelle forme e modalità nonché attraverso i mezzi ritenuti più idonei.

RESPONSABILE DELLA PROTEZIONE DEI DATI

ALLEGATO A)1

NOMINA A RESPONSABILE DEL TRATTAMENTO

Nel rispetto di quanto previsto dall'articolo 37 del GDPR, il Responsabile della Protezione Dati (in seguito **RPD**) viene nominato l'**Avv. STEFANO ASCIONI,** che ha in essere un rapporto di collaborazione coordinata e continuativa con l'APT. Il già menzionato professionista è in possesso 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 costituirà presso l'APT una figura di riferimento per tutte le questioni di carattere generale riguardanti la protezione dei dati personali.
Al RPD sono affidati i seguenti compiti:
a) supportare, informare e fornire consulenza al Titolare 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'articolo 30 del GDPR, coordinando le attività di compilazione 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 dell'APT;
d) informare e fornire consulenza al Titolare 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* dell'APT in cui vengano assunte decisioni relative al trattamento dei dati personali;
e) sorvegliare e valutare l'osservanza del GDPR 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 articoli 35 e ss. del GDPR, 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'APT, supportando il soggetto competente – secondo quanto previsto in appositi atti interni – nelle decisioni circa:

- provvedere alla gestione delle notificazioni e comunicazioni dei data BREACH di cui agli articoli 33 e 34 del GDPR;
- la segnalazione di tali violazioni, 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 GDPR;
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 dell'APT rientrante nelle attività della stessa APT; se del caso potrà svolgere attività di formazione introduttiva al personale sulle principali tematiche del GDPR;
i) provvedere alla istituzione, alimentazione e aggiornamento del Registro delle richieste di esercizio dei diritti degli interessati.

I compiti dell'RPD attengono all'insieme dei trattamenti di dati effettuati dall'APT e comprendono:

1. tutti i trattamenti di dati personali gestiti dall'APT sia presso la sede centrale che presso altre sedi, compresa l'attività eventualmente delegata a soggetti esterni;
2. la vigilanza su eventuali trattamenti svolti, su incarico dell'APT, da Aziende speciali o Società in house o uffici del Comune di Livigno.

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) a 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 riferirà direttamente al Titolare, con possibilità di esprimere le sue valutazioni quando lo riterrà opportuno o si renderà necessario, o quando gli verrà espressamente richiesto.

Il RPD potrà essere convocato dal Consiglio, 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 MOP, al RPD sono attribuiti i seguenti poteri e prerogative, in assenza di qualsivoglia istruzione (come stabilito dall'art. 38, comma 3, GDPR):

a) l'APT 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 amministrativo del RPD nelle attività che esso dovrà svolgere, e un referente tecnico/informatico 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'APT;
b) l'APT 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 struttura dell'APT, 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'APT deve mettere a disposizione una specifica casella di posta elettronica dpo@livigno.eu 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; l'accesso sarà riservato esclusivamente al RPD;

f) i dati di contatto del RPD (recapito postale, telefono, e-mail), comunicati al Garante per la protezione dei dati personali, sono resi disponibili, a esclusione del suo nominativo, sul sito *internet* istituzionale dell'APT, e riportati nelle informative rese agli interessati;
g) al RPD sono inoltre riconosciuti, per effetto del presente atto anche il potere di autoregolamentazione, in forza del quale il RPD:
1) 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;
2) poteri ispettivi, in forza dei quali, nell'esercizio delle proprie funzioni di controllo, il RPD potrà:

- utilizzare le risultanze delle attività ispettive e svolgere autonomamente verifiche anche a sorpresa;
- accedere liberamente a ogni documento rilevante per lo svolgimento delle sue funzioni;
- disporre l'acquisizione di informazioni, dati e/o notizie a semplice richiesta, senza preventiva autorizzazione;
- richiedere l'audizione ovvero il coinvolgimento nelle attività di verifica di qualsivoglia dipendente dell'APT.

REFERENTI PRIVACY

ALLEGATO A)2

NOMINA A REFERENTI PRIVACY

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

SOGGETTI AUTORIZZATI AL TRATTAMENTO

ALLEGATO A)3

NOMINA QUALE PERSONA AUTORIZZATA AL TRATTAMENTO DATI

L'art. 4, punto 10, del GDPR 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 GDPR, 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 Codice, 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 Titolare autorizza, con la stessa nota di incarico, i Responsabili delle unità organizzative, quali "*Autorizzati Responsabili*", al trattamento dei dati pertinenti al settore di responsabilità affidato, con assegnazione di specifiche istruzioni che devono avere come contenuto minimo quelle indicate nel presente MOP.
Inoltre, il Titolare autorizza i dipendenti indicati dai Responsabili delle unità organizzative quali "*Autorizzati Responsabili*", al trattamento dei dati pertinenti al settore di operatività.
I Responsabili hanno cura di consegnare a loro volta le già menzionate istruzioni ai dipendenti incardinati negli uffici sottoposti alla loro responsabilità che si considerano, in automatico, in forza del presente MOP, e secondo gli ordini di servizio che dispongono la mobilità interna, soggetti "*Autorizzati".*

I soggetti così Autorizzati svolgono i trattamenti "*per conto*" del Titolare e sono formalmente autorizzati anche per *RELATIONEM* con rinvio al presente MOP e al Registro dei Trattamenti.
Il personale autorizzato deve effettuare le operazioni di trattamento secondo le istruzioni impartite dal Titolare Nello specifico, i soggetti Autorizzati dovranno:
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 predisposti da ciascun ufficio competente, 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'APT;
10) rispettare le disposizioni impartite per iscritto dal 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* e dal MOP per l'utilizzo degli strumenti informatici e delle misure di sicurezza, 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 camerali; 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 potesse derivare una interruzione del servizio pubblico che l'APT 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'APT;
- 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;
- comunicare al RPD 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 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*);
- collaborare più in generale con il RPD provvedendo a fornire ogni informazione da questi richiesta.

In aggiunta alle già menzionate istruzioni, 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.
Le istruzioni sopra elencate sono quelle minime da rispettare. I soggetti Autorizzati Responsabili possono proporre al Titolare l'adozione di ulteriori istruzioni in relazione agli specifici trattamenti curati dal servizio di competenza o chiedere di integrare le istruzioni per le specifiche esigenze dell'Area di competenza.
Qualora si rendesse necessario derogare o modificare le istruzioni minime in parola, i soggetti Autorizzati Responsabili dovranno darne apposita motivazione e puntuale giustificazione.
Il mancato rispetto delle istruzioni impartite a tutela della *privacy* potrebbe comportare l'insorgere di responsabilità dell'APT con conseguente possibile contestazione disciplinare, in base al vigente CCNL, a carico del dipendente.

AMMINISTRATORE DEL SISTEMA

ALLEGATO A)4
NOMINA AMMINISTRATORE DI SISTEMA

ALLEGATO A)5
NOMINA AMMINISTRATORE DI SISTEMA ESTERNO

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 successive ed integrazioni 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'APT procede alla nomina dei necessari Amministratori di Sistema, i cui compiti, specificatamente e limitatamente a tale contesto, consistono in:
a) assicurare la corretta custodia delle credenziali per la gestione dei sistemi di autenticazione e di autorizzazione in uso in ambito camerale, anche impartendo apposite istruzioni agli incaricati del trattamento che utilizzino strumenti elettronici;
b) predisporre e rendere funzionanti le copie di sicurezza (operazioni di *BACKUP* e *DISASTER RECOVERY)* dei dati e delle applicazioni;
c) 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;
d) relazionare, periodicamente, circa l'attività svolta e lo stato di attuazione delle politiche in tema di protezione dei dati personali, segnalando eventuali criticità.

RESPONSABILE ESTERNO DEL TRATTAMENTO

ALLEGATO A)6

NOMINA RESPONSABILE ESTERNO AL TRATTAMENTO DATI

A norma dell'articolo 28 del GDPR, l'APT 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 GDPR, con particolare riferimento alla 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'APT è Titolare.
L'incarico come Responsabile può essere disposto direttamente dal Titolare, con propria determinazione o dai Responsabili unità organizzative e in tal caso, il Responsabile informa il Titolare, al fine di consentire allo stesso 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 al provvedimento amministrativo che vincoli il Responsabile stesso al Titolare del trattamento e che definisca 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 dovrà, inoltre, prevedere, quale contenuto minimo, le prescrizioni e gli obblighi appresso indicati:
1) effettuare il trattamento dei dati personali in modo lecito e secondo correttezza nel rispetto delle istruzioni del Titolare delle disposizioni contenute nel GDPR e nei provvedimenti del Garante della *Privacy*;
2) 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;

3) adottare tutte le necessarie e appropriate misure di sicurezza tecniche e organizzative così come disciplinate dal GDPR, tenendo conto del rischio per i diritti e le libertà delle persone fisiche, e mettere in atto le predette misure al fine di garantire un livello di sicurezza adeguato 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, al qual proposito, il Responsabile deve garantire, e il Titolare ne prenderà atto, di essere dotato di un proprio Sistema di gestione della sicurezza delle informazioni in costante aggiornamento in relazione allo stato del progresso tecnico;

4) provvedere, in particolare, ad attivare le seguenti misure minime di sicurezza:

- 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;

5) 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, nonché informare il Titolare qualora, a suo parere, un'istruzione violi disposizioni relative alla protezione dei dati;

6) attuare un controllo sull'attività svolta dalle persone autorizzate al trattamento al fine di verificare l'effettivo rispetto da parte di questi ultimi delle misure di sicurezza adottate e, comunque, delle istruzioni impartite;

7) fornire 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;

8) 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 già menzionate comunicazioni nonché gli adempimenti previsti dalla normativa vigente in materia di protezione dei dati personali sono di competenza del Titolare;

9) 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;

10) assistere il Titolare, tenendo conto della natura del trattamento, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato per quanto previsto nella normativa vigente;

11) in caso di violazione di dati personali, informare il Titolare del trattamento senza ritardo - e comunque entro quarantotto ore dal momento in cui è venuta a conoscenza della violazione - e collaborare attivamente con il Titolare stesso, nella raccolta documentale e in tutte le attività connesse all'eventuale notifica al Garante Privacy e ai soggetti interessati, per quanto previsto nella normativa vigente;

12) assistere il Titolare del trattamento nel garantire il rispetto degli obblighi, previsti dal GDPR, relativamente all'attuazione delle misure di sicurezza, alla comunicazione in caso di violazione dei dati personali e alla valutazione di impatto sulla protezione dei dati tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
13) fornire al Titolare, a semplice richiesta e secondo le modalità indicate da quest'ultimo, i dati e le informazioni necessari 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;
14) compiere tempestivamente quanto necessario per conformarsi a richieste pervenute dal Garante o dall'Autorità Giudiziaria o, comunque, dalle Forze dell'Ordine;
15) mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dal GDPR e il rispetto degli obblighi di cui all'atto di nomina, consentendo e contribuendo alle attività di revisione, comprese le ispezioni realizzate dal Titolare (o da un altro soggetto da questi incaricato);
16) 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.
17) relativamente a quanto prescritto dal Provvedimento del Garante del 27 novembre 2008 relativo alle "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema",* al Responsabile del trattamento sono attribuite le attività di valutazione, designazione, verifica attività e registrazione degli accessi degli amministratori di sistema e pertanto lo stesso ha l'obbligo di:

- procedere alla designazione individuale degli amministratori di sistema o figura equivalente, 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;
- riportare, per ciascun amministratore di sistema designato, o figura equivalente, l'elencazione degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;
- conservare gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema o figura equivalente;
- verificare, con cadenza almeno annuale, l'operato degli amministratori di sistema o figure equivalenti in modo da controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza per il trattamento dei dati personali previste dalle norme vigenti;
- adottare sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema o figure equivalenti; le registrazioni dovranno essere conservate per un congruo periodo, comunque non inferiore a sei mesi.

Ogni specifico atto di incarico potrà prevedere prescrizioni aggiuntive in relazione alla specificità del trattamento effettuato dal Responsabile per conto dell'APT.
Qualora si rendesse necessario derogare o modificare tali prescrizioni, l'atto di incarico deve contenere apposita motivazione e puntuale giustificazione.
I Responsabili del Trattamento come sopra nominati sono autorizzati in forza del presente MOP, a norma dell'art. 28, comma 2, del GDPR a ricorrere, se necessario per l'espletamento delle forniture e dei compiti assegnati, a ulteriori eventuali Responsabili del trattamento per specifiche attività di trattamento trasferendo su di essi le disposizioni del Titolare e adottando opportune clausole contrattuali al fine di richiamare l'obbligo in capo ai medesimi di rispettare le misure di sicurezza descritte nell'atto di nomina. La nomina di ulteriori Responsabili deve essere comunicata al Titolare, ove richiesto.

FORNITORI – CONSULENTI – COLLABORATORI – INCARICATI A QUALSIASI TITOLO

Ai fornitori, consulenti, collaboratori e a qualsiasi altro soggetto incaricato dall'APT 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'APT, 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 dell'APT:

- 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 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:

a) per i dipendenti che dovranno coadiuvare i soggetti previsti dal presente MOP per gli adempimenti di propria competenza, ferme restando le relative responsabilità in capo a questi ultimi;
b) 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 dai delegati del Titolare. L'organizzazione di tali percorsi ed eventuali specifiche azioni formative

- saranno progettati e gestiti operativamente dal Servizio competente in materia di personale, in accordo con il Titolare e il RPD;
- saranno monitorate dal RPD sia per quanto riguarda la realizzazione che gli esiti.

I dipendenti e collaboratori dell'APT potranno 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. È sempre diretta la possibilità di contattare l'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.

GDPR E WHISTLEBLOWING

La Direttiva Whistleblowing è la dicitura con cui viene più comunemente indicata la Direttiva Europea 2019/1937 sulla "Protezione delle Persone che Segnalano Violazioni del Diritto dell'Unione" recepita dall'Italia con il D.lgs. 24/2023.
Tale direttiva, la cui applicazione è obbligatoria per tutte le aziende pubbliche nonché quelle private con più di 50 dipendenti, prevede lo sviluppo di un sistema volto a:
Tutelare "chi, dopo aver constatato illeciti nell'organizzazione, denuncia l'illecito per dovere civico" (il c.d. *whistleblower*)
Agevolare le segnalazioni garantendo riservatezza al segnalante

Permettere alle organizzazioni di rientrare in contatto con il segnalante al fine di ottenere eventuali maggiori informazioni necessarie per gestire le segnalazioni ricevute e intervenire correttamente sulla situazione
Anche le attività richieste dalla Direttiva Whistleblowing, per essere a norma di legge, devono essere svolte e impostate nel rispetto del Regolamento Europeo per la Protezione dei Dati Personali (GDPR, detto anche Regolamento Privacy).
In particolare, l'organizzazione che attua la Direttiva nel rispetto della normativa privacy deve svolgere i seguenti adempimenti:
Registrare il relativo trattamento dati nel Registro dei Trattamenti. Il trattamento deve essere stato progettato fin dall'inizio nel rispetto dei principi imposti dal Regolamento
Fornire a dipendenti, collaboratori, azionisti ecc. un'apposita Informativa Privacy al fine di renderli consapevoli a priori di come verrebbero trattati i loro dati nel momento in cui decidessero di effettuare una segnalazione
Eseguire una DPIA (DATA PROTECTION IMPACT ASSESSMENT), in italiano "Valutazione di Impatto sulla Protezione dei Dati Personali". Si tratta di un'attività richiesta dal GDPR ogni volta che il trattamento può comportare un rischio elevato per i diritti e le libertà delle persone, come nel caso delle attività di whistleblowing. In particolare, una DPIA serve a descrivere il trattamento, valutarne la necessità e la proporzionalità nonché a determinare come gestire gli eventuali rischi per i diritti e le libertà delle persone derivanti dal trattamento.
Fornire e far sottoscrivere un'apposita lettera di Autorizzazione al Trattamento ai dipendenti chiamati a gestire il canale di segnalazione
Nell'ipotesi in cui l'azienda si avvalesse di fornitori terzi per la gestione del canale di segnalazione (es. fornitore di un software terzo), designare tali fornitori come "Responsabili del Trattamento" Nel caso di realtà che decidono di condividere il sistema per il ricevimento e la gestione delle segnalazioni, stipulare un accordo interno con gli altri contitolari del trattamento per definire le rispettive responsabilità.

ADEMPIMENTI NECESSARI

Per la conformità al GDPR, enti ed organizzazioni devono configurare un c.d. «sistema privacy», che si evolve nel tempo, costituito dai seguenti componenti:

1. Informative
2. Lettere di Designazione
3. Procedure
4. Registro DATA BREACH
5. Analisi dei Rischi
6. Privacy by Design e DPIA

Informative
Ai sensi del GDPR, il Titolare adotta misure appropriate per fornire all'interessato (utente, cliente, dipendente o PROSPECT) tutte le informazioni relative al trattamento. Mediante l'impiego dell'informativa il Titolare fornisce agli Interessati tutte le informazioni relative ai trattamenti eseguiti in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici.
Fra le informative ricordiamo quelle rivolte all'utente, alla clientela, ai dipendenti e il cookie policy.
L'informativa deve contenere almeno:

- identità del Titolare;
- dati dei Responsabili e dei Destinatari del Trattamento;
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- eventuali legittimi interessi perseguiti;

- eventuali trasferimenti di dati all'estero;
- il periodo di conservazione dei dati personali;
- diritti degli interessati esercitabili;
- eventuale trattamento di dati particolari;
- la natura del conferimento (obbligatorio o meno);
- eventuale presenza di processi decisionali automatizzati compresa la profilazione.

Lettere di Designazione

Ai sensi dell'art. 29 del GDPR chiunque tratta dati personali per conto del Titolare del Trattamento deve ricevere specifiche istruzioni.

Il Titolare può ricorrere a:

- Responsabili del Trattamento, in genere fornitori a cui il Titolare affida i dati personali;
- Soggetti Autorizzati (persone fisiche, compresi gli Amministratori di Sistema, ex. Incaricati), costituiti in genere dai dipendenti del Titolare a cui vengono attribuiti i privilegi di accesso per accedere ai dati.

Le designazioni di Responsabili ed Autorizzati sono in genere redatte in forma scritta mediante specifiche lettere con termini appropriati.

Procedure

Il Titolare del Trattamento regola la propria attività mediante specifiche procedure ai fini di dimostrare la conformità al GDPR:

- Privacy by Design / Default e DPIA.
- Gestione delle violazioni dei Dati personali (DATA BREACH); Gestione esercizio Diritti interessati.
- Processo per la nomina di Responsabili del Trattamento.
- Processo per la nomina di Soggetti Autorizzati (Ex. Incaricati).
- Processo per la conservazione e cancellazione dei dati personali

Analisi dei Rischi

L'articolo 32 del GDPR, afferma che: "Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, 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:

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento."

L'approccio che ogni Titolare del trattamento deve seguire, per il trattamento dei dati personali, deve essere basato sul rischio: più alto è il rischio e più severe devono essere le misure che il Titolare o il Responsabile del trattamento devono considerare mitigare il rischio.

A tal fine sia il Titolare che il Responsabile devono configurare, in relazione ai trattamenti eseguiti un modello per la determinazione dei rischi per le libertà e i diritti degli interessati considerando:

- L'impatto per gli interessati a seguito di una violazione che riguarda la riservatezza, integrità, disponibilità dei dati nonché aspetti critici del trattamento eseguito;
- Le minacce che possono insistere sui trattamenti;
- Le misure di mitigazione delle minacce che possono insistere sui trattamenti

Privacy by Design / Default e DPIA

Il GDPR disciplina il concetto di Privacy by Design all'art. 25 "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita".

Ai sensi di tale disposizione, il Titolare del Trattamento ha il dovere di adottare misure tecniche e organizzative adeguate al fine di dare concreta attuazione alle disposizioni ed ai principi in materia di protezione dei dati (in particolare la minimizzazione), garantendo la conformità ai requisiti del regolamento ed un efficace esercizio dei diritti degli Interessati. A tale riguardo bisognerà tenere conto:

- dello stato dell'arte e costi di implementazione di ogni misura;
- della natura, contesto, ambito di applicazione e finalità del trattamento in progetto;
- dei rischi (e connessa probabilità e gravità degli stessi) che il trattamento potrebbe porre per le libertà e i diritti degli Interessati.

Il progetto (applicazione o procedura organizzativa) che prevede l'istituzione e/o la modifica sostanziale di un trattamento, avendo come punto di riferimento il principio di "Privacy by Design", è da implementare in modo tale da porre particolare attenzione alla gestione dell'intero ciclo di vita dei dati personali, alla raccolta e alla cancellazione degli stessi con specifico riguardo alle garanzie procedurali in merito all'esattezza, alla riservatezza, all'integrità, alla sicurezza fisica e alla cancellazione dei dati personali.

All'interno del processo di Privacy by Design, se il trattamento dovesse presentare rischi elevati per gli interessati, il Titolare del Trattamento è tenuto alla esecuzione di un DPIA

Il GDPR impone ai Titolari del Trattamento l'esecuzione della DPIA (DATA PROTECTION IMPACT ASSESSMENT), cioè una valutazione d'impatto ai fini privacy, per tutti quei trattamenti che possano "...presentare un rischio elevato per i diritti e le libertà delle persone fisiche" in considerazione della natura, dell'oggetto, del contesto e delle finalità.

La DPIA è una valutazione che deve essere condotta seguendo specifiche metodologie (vedi provvedimento WP 248); l'articolo 35 del GDPR definisce la DPIA come uno strumento che, in ossequio al principio di accountability, consente ai titolari di dimostrare di aver adottato misure appropriate nelle attività di trattamento.

La conformità al GDPR è un percorso che non si esaurisce con la semplice redazione di informative da sottoporre alla firma degli interessati.

Sistema di monitoraggio

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 e 32 del GDPR.

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

a) controllo di primo livello (c.d. "controllo di linea"), posto in essere dai dirigenti ("Delegati del Titolare") coadiuvati dai responsabili delle unità organizzative ("Autorizzati Responsabili" nell'ambito delle ordinarie funzioni di coordinamento e gestione delle attività di propria competenza;

b) 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**: Ai sensi dell'Art. 33 c.5 del GDPR "Il Titolare del Trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

Il Titolare del Trattamento deve tenere un registro preposto alla registrazione delle violazioni dei dati personali in cui annotare tutte le violazioni avvenute comprese quelle che non vanno notificate al Garante Privacy cioè quelle che non hanno un rischio elevato per le libertà e i diritti degli interessati.

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 GDPR. 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 di cui all'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;
- 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 de conseguente verifica dello scostamento rispetto ai valori obiettivo ivi definiti (da considerarsi quali "ALERT" ovvero indici di situazioni di rischio potenziale).

FLUSSI INFORMATIVI

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	Responsabile Attività Negoziale
Tempestiva	Sanzioni comminate da Pubbliche autorità in materia di privacy	Responsabile Attività Negoziale
Tempestiva	Copia relazioni / verbali redatti in sede di audit di I livello in cui si evidenzino criticità lato privacy	Delegati del Titolare
Quadrimestrale	Schede di rilevazione eventi	Delegati del Titolare
Quadrimestrale	Verbali di analisi degli incidenti (cfr. procedura di data	Delegati del Titolare
Quadrimestrale	Risposte agli interessati in caso di reclami/esercizio diritti	Delegati del Titolare
Tempestiva	Informativa relativa al rifiuto di assunzione del ruolo/designazione a Responsabile esterno del trattamento	Delegati del Titolare

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 paragrafo 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
COMPLIANCE ALLA NORMATIVA	Numero di richieste/reclami con identico oggetto o relative ad uno stesso trattamento	>3	Registro delle richieste di esercizio dei diritti
COMPLIANCE ALLA NORMATIVA	Tempi di risposta alle richieste di esercizio dei diritti da parte degli interessati	< 30gg -	Registro delle richieste di esercizio dei diritti
COMPLIANCE ALLA NORMATIVA	Numero di ispezioni subite da pubbliche autorità su segnalazione/denuncia degli interessati nell'anno	>1	Flussi informativi al RPD
COMPLIANCE ALLA NORMATIVA	Numero di sanzioni comminate in materia da pubbliche autorità nell'anno	>0	Flussi informativi al RPD
COMPLIANCE ALLA NORMATIVA	Numero di soggetti esterni che hanno rifiutato la designazione a Responsabile esterno del trattamento	>2	Flussi informativi al RPD

DIMENSIONE DEL MONITORAGGIO	DESCRIZIONE INDICATORE	VALORE SEGNALETICO	FONTE DI REPERIMENTO DEL DATO
CONTROLLO E MIGLIORAMENTO CONTINUO	Numero di privacy audit effettuati nell'anno	< 1 -	Verbali/relazioni di audit/ Relazioni agli Organi
CONTROLLO E MIGLIORAMENTO CONTINUO	% di Non Conformità (NC) riscontrate (n. NC / n. audit)	> 20% -	Verbali/relazioni di audit/ Relazioni agli Organi
CONTROLLO E MIGLIORAMENTO CONMTINUO	Numero di data BREACH notificati al Garante oltre i termini previsti dal GDPR (72h)	< 30gg -	Relazione agli Organi

DIMENSIONE DEL MONITORAGGIO	DESCRIZIONE INDICATORE	VALORE SEGNALETICO	FONTE DI REPERIMENTO DEL DATO
SICUREZZA E DISPONIBILITA' DEI DATI	Numero di segnalazioni di incidenti inserite nel Registro dei Data BREACH	> 3/anno -	Registro data BREACH
SICUREZZA E DISPONIBILITA' DEI DATI	Numero di violazioni di dati personali notificate al Garante Privacy ex art. 33 GDPR	> 1	Registro data BREACH

SICUREZZA E DISPONIBILITA' DEI DATI	Numero di data BREACH notificati al Garante oltre i termini previsti dal GDPR (72h)	>1	Registro data BREACH

DIMENSIONE DEL MONITORAGGIO	**DESCRIZIONE INDICATORE**	**VALORE SEGNALETICO**	**FONTE DI REPERIMENTO DEL DATO**
SICUREZZA E DISPONIBILITA' DEI DATI	Numero di violazioni di dati personali comunicate agli interessati ex art. 34 GDPR	> 1	Registro data BREACH
SICUREZZA E DISPONIBILITA' DEI DATI	Tempi medi di risoluzione incidenti e problematiche di sicurezza (sommatoria giorni tra segnalazione e risoluzione / numero segnalazioni)	> 7 -	Sistema ticketing interno / fornitori esterni
SICUREZZA E DISPONIBILITA' DEI DATI	Tempi medi di risoluzione incidenti bloccanti (sommatoria giorni tra segnalazione e risoluzione / numero segnalazioni)	> 2 -	Sistema ticketing interno / fornitori esterni

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.

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

RIESAME 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 Camerale;
- 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 alla Giunta Camerale per l'assunzione delle eventuali decisioni necessarie a garantire la compliance e il miglioramento continuo.

SINTESI RUOLI

TITOLARE DEL TRATTAMENTO

Il titolare del trattamento è l'**AZIENDA DI PROMOZIONE E SVILUPPO TURISTICO DI LIVIGNO S.R.L.,** con sede in 23030 Livigno (SO) Via Via RASIA n. 999 (23041) – codice fiscale/ partita IVA n. 92015260141 - in persona del Sig. **LUCA MORETTI**, nella sua qualità di Presidente del Consiglio di Amministrazione. I dati di contatto del titolare sono:

I dati di contatto del titolare sono:
Telefono: +39 0342 977810
Cellulare: +39 346 7371877
e-mail: luca.moretti@livigno.eu
PEC: luca.moretti@pec.livignocert.eu
Titolare del trattamento è la persona fisica o giuridica che «determina le finalità e i mezzi del trattamento di dati personali» (articolo 4, n. 7 del GDPR).

RESPONSABILE DELLA PROTEZIONE DEI DATI

Il responsabile della protezione dei dati (RPD) del l'**AZIENDA DI PROMOZIONE E SVILUPPO TURISTICO DI LIVIGNO S.R.L.** è l'Avv. **STEFANO ASCIONI**
Al responsabile per la protezione dei dati sono demandati i compiti di cui all'art. 39 del GDPR. Tra i quali spiccano, per importanza, quello di «fornire consulenza al titolare del trattamento [...] nonché ai dipendenti che

eseguono il trattamento», di «sorvegliare l'osservanza del [...] regolamento», di «cooperare con l'autorità e fungere da punto di contatto con l'autorità di controllo».
Gli interessati, ossia le persone fisiche cui i dati si riferiscono, «possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal [...] regolamento» (articolo 38, paragrafo 4 del GDPR).
Nella specie, le persone fisiche interessate ad attività di trattamento eseguite dall'**AZIENDA DI PROMOZIONE E SVILUPPO TURISTICO DI LIVIGNO S.R.L.** – esemplificativamente il personale tecnico-amministrativo – possono contattare il RPD al seguente indirizzo:
Cellulare: + 39 3485113441
e-mail: info@studioascioni.it
PEC: rup.ascionistefano@pec.it
Per "*violazione dei dati personali*" (c.d. *DATA BREACH*) s'intende «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» (art. 4, n. 12. del GDPR).
È possibile approfondire la materia del *DATA BREACH* accedendo alla seguente pagina del sito istituzionale del Garante per la protezione dei dati personali: https://www.garanteprivacy.it/regolamentoue/databreach.
Per segnalare eventuali violazioni al trattamento dei dati personali, chiunque può rivolgersi al servizio di *DATA BREACH* dell''**AZIENDA DI PROMOZIONE E SVILUPPO TURISTICO DI LIVIGNO S.R.L**, raggiungibile all'indirizzo: privacypec.livignocert.eu

GRUPPO DI LAVORO INTERDISCIPLINARI

Il titolare del trattamento e il responsabile della protezione dei dati dell''**AZIENDA DI PROMOZIONE E SVILUPPO TURISTICO DI LIVIGNO S.R.L**, sono supportati da un gruppo di lavoro interdisciplinari, nei quali convergono professionalità informatiche e amministrative.
Il gruppo di lavoro è costituito dai Responsabili di settore e precisamente: ANNA SPANDRI e RUDY GURINI
Il gruppo di lavoro è disponibile per chiarimenti o delucidazioni sull'applicazione della normativa all'interno dell''**AZIENDA DI PROMOZIONE E SVILUPPO TURISTICO DI LIVIGNO S.R.L** e possono essere contattati all'indirizzo e-mail:
anna.spandri@livigno.eu,
rudy.gurini@livigno.eu.

AMMINISTRATORIE DI SISTEMA

Sono stati nominati Amministratori di sistema dell''**AZIENDA DI PROMOZIONE E SVILUPPO TURISTICO DI LIVIGNO S.R.L**, il signor Rudy Gurini rudy.gurini@livigno.eu.

RESPONSABILE ESTERNO

Sono stati identificati dei responsabili esterni all'azienda relativamente ad aree specifiche, a supporto delle attività del titolare del trattamento, del responsabile della protezione dei dati dell''**AZIENDA DI PROMOZIONE E SVILUPPO TURISTICO DI LIVIGNO S.R.L** e dell'amministratore di sistema.
⇒ Per il trattamento dei soli dati necessari alla manutenzione e aggiornamento dell'infrastruttura di rete, della gestione e manutenzione dei server, della gestione e manutenzione di macchine virtuali, degli applicativi di cybersecurity e accesso remoto è stata identificata l'azienda INTELLOPE S.R.O. con sede principale in Slovacchia.
⇒ Per il trattamento dei soli dati necessari alla manutenzione dei sistemi di domotica, di videosorveglianza e di allarme installati presso le varie strutture è stata identificata l'azienda NEW ELETTRA S.R.L. con sede in Livigno nella persona del Sig. Bracchi Matteo
⇒ Per il trattamento dei soli dati necessari alla manutenzione dell'infrastruttura server cloud fornita per gli applicativi di ERP e HR in uso, è stata identificata l'azienda NOVUS S.R.L. con sede a Desio (MB) nella persona del Dott. Emanuele Capiaghi

⇒ Per il trattamento dei soli dati necessari alla consulenza e allo sviluppo di soluzioni web (siti web, comunicazione online) è stata identificata l'azienda ALEA PRO S.N.C. con sede a Pordenone (PN) nella persona del Dott. Cristian Fiorot

⇒ Per il trattamento dei soli dati necessari alla consulenza e allo sviluppo dell'app MYLIVIGNO è stata identificata l'azienda WEDIGITAL S.R.L. con sede a Pordenone nella persona del Dott. Cristian Fiorot.

⇒ Per il trattamento dei soli dati necessari alla manutenzione, gestione, sviluppo ed interfacciamento della piattaforma di prenotazione e promo commercializzazione delle disponibilità delle strutture ricettive operanti a Livigno, è stata identificata l'azienda YANOVIS S.R.L. son sede a Bolzano (BZ) nella persona del Dott. Patrick Bergmeister.

⇒ Per il trattamento dei soli dati necessari alla configurazione, manutenzione ed assistenza relativa all'utilizzo della piattaforma ZMENU, sono state identificate le aziende ZUCCHETTI S.P.A. e FUTURA ICT S.R.L. con sede a Sondrio nella persona del Dott. Matteo Morelli

⇒ Per il trattamento dei soli dati necessari alla configurazione, manutenzione, gestione ed assistenza relativi all'utilizzo della piattaforma WELLBY, è stata identificata l'azienda ZUCCHETTI HOSPITALITY S.R.L. con sede a Lodi nella persona del Sig. Marco Stefanon.

⇒ Per il trattamento dei soli dati necessari alla gestione degli apparati e dei servizi di connettività/fonia, sono state identificate le aziende FASTWEB S.P.A., con sede a Milano nella persona del Sig. Andrea Ballan GLOBALTEL S.R.L. con sede a Sondrio nella persona del Sig. Sergio Almacci, INTRED S.P.A. con sede a Brescia nella persona del Sig. Egon Zanagnolo, FLAN S.N.C. con sede a Livigno nella persona del Sig. Flavio Cantoni.

⇒ Per il trattamento dei soli dati necessari alla gestione dei dati relativi alla realizzazione e comunicazione di dati relativi a bollettini valanghe e qualità neve, è stata identificata l'azienda ALPSOLUT S.R.L. con sede a Livigno nella persona del Dott. Fabiano Monti.

⇒ per il trattamento dei soli dati necessari relativi agli adempimenti obbligatori previsti dall'Art. 25 Dlgs 81/2008 – TUSL in materia di igiene e sicurezza nei luoghi di lavoro: il Dott. Paolo Gasperi

⇒ per il trattamento dei soli dati necessari relativi allo svolgimento di investigazioni difensive o per far valere o difendere in sede giudiziaria un diritto in nome e per conto dello scrivente Titolare: Studio Legale Avv. STEFANO ASCIONI

L'elenco aggiornato di tutti i Responsabili per il trattamento dei dati personali, da noi nominati, con l'indicazione delle relative responsabilità è reperibile contattando il signor Luca Moretti.

ELENCO DEI TRATTAMENTI DI DATI PERSONALI EFFETTUATI

In questa sezione è descritto il trattamento realizzato, in modo da consentire una valutazione di adeguatezza delle misure adottate per garantire la sicurezza del trattamento. In tale descrizione sono precisate le finalità del trattamento, le categorie di persone interessate e dei dati o delle categorie di dati relativi alle medesime, i destinatari o le categorie di destinatari a cui i dati possono essere comunicati nonché la descrizione degli strumenti utilizzati.

Identificativo T del trattamento	**Finalità perseguita**	**Categorie di Interessati**	**Natura dei dati trattati**	**Destinatari o categorie di destinatari a cui i dati possono essere comunicati**	**Descrizione degli strumenti utilizzati**
T1	Gestione forniture	Fornitori	Dati di natura comune	Consulenti per adempiere e Autorità Pubbliche	Posta elettronica – piattaforma e-procurement

T2	Gestione contratti Clienti	Clienti	Dati di natura comune e sensibile		Posta elettronica – pec aziendale -
T3	Gestione del Personale	Dipendenti/Collaboratori	Dati di natura comune e sensibile	Consulenti per adempiere e Autorità Pubbliche	Comunicazioni a mezzo pec personale

MANSIONARIO PRIVACY

In questa sezione è riportato l'elenco, anche per categorie, degli incaricati del trattamento e delle relative responsabilità. Le modalità attraverso le quali è possibile individuare l'elenco aggiornato dei responsabili del trattamento con le relative responsabilità è indicata al termine della Sezione II del presente Documento.
Le Unità organizzative nelle quali vengono effettuati i trattamenti di dati personali sono le seguenti:
U1: Ufficio Amministrativo;
U2: Ufficio Marketing;
U3: Ufficio Eventi
U4: Ufficio Booking
U5: MyLivignoTv
U6: Museo MUS
U7: Aquagranda
U8: ITC
U9: Ufficio informazioni

Nominativi degli Incaricati al trattamento e relative Unità organizzative d'appartenenza

U1	**Ufficio Amministrativo/Personale**	**Ing. Anna Spandri**
U2	**Ufficio Marketing**	**Michela Martinelli**
U3	**Ufficio Evnti**	**Thomas Confortola**
U4	**Ufficio Booking**	**Sara Gianoncelli**
U5	**MyLivignoTV**	**Sara Bovo**
U6	**Museo MUS**	**Desirè Castellani**
U7	**Aquagranda**	**Veronica Martinelli**
U8	**ITC**	**Rudy Gurini**
U9	**Ufficio Informazioni**	**Anne Fey**

Competenze e responsabilità delle Unità organizzative

Unità Organizzativa	Trattamento Effettuato "T"	Acquisizione e caricamento dei dati	Consultazione	Comunicazione a Terzi	Manutenzione tecnica dei programmi	Gestione tecnica Operativa della base Dati (salvataggi, ripristini etc.)
U1	si	si	si	si	-	si
U2	si	si	si	si	-	Si
U3	si	si	si	si	-	Si

U4	si	si	si	si		Si
U5	si	si	si	si	Si	Si
U6	si	si	si	si	-	Si
U7	si	si	si	si	-	si
U8	si	si	no	no	si	si
U9	si	si	si	si	-	si

INFORMATIVE/CONSENSO

Il GDPR prevede che il «titolare del trattamento adotti[*i*] misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 [...] in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro».
La tutela del dato sensibile prevale su una generica esigenza di trasparenza amministrativa sia sotto il profilo costituzionalmente rilevante della valutazione degli interessi in discussione sia sotto quello della sostanziale elusione della normativa sulla protezione dei dati personali, accentuata nel caso dei dati sensibili, ove si dovesse far prevalere una generica esigenza di trasparenza amministrativa nemmeno concretamente argomentata e provata.
Peraltro, nella nozione di trattamento, ai sensi dell'art. 4 I lettera a) del codice della privacy, sono compresi l'estrazione dei dati ed il successivo utilizzo.
Queste attività, se non precedute da idonea informativa sul trattamento dei dati personali e dalla acquisizione del consenso del titolare, integrano due illeciti amministrativi previsti dagli artt. 13, 23, 130,161, 162 c. 2 bis e 167 del codice della privacy, riferiti alla omessa informativa ed alla non assentita comunicazione automatizzata. Inoltre, è consolidato il principio che i dati sensibili idonei a rilevare lo stato di salute possono essere trattati dai soggetti pubblici soltanto mediante modalità organizzative che rendano non identificabile l'interessato. Il consenso a uno specifico trattamento di dati personali per essere valido deve essere prestato in maniera espressa, libera e specifica.
Ciò significa che è legittimo il trattamento di dati personali solo se fondato su un consenso del singolo puntuale e specificatamente riferito alle modalità trattamentali previste.

MISURE DI SICUREZZA

In questa sezione sono descritte le misure di sicurezza adottate per prevenire:
⇒ 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.

Misure di sicurezza adottate o da adottare

Misure	Descrizione dei rischi contrastanti	Trattamenti interessati	Misure in essere	Misure adottate/ da adottare e tempi previsti	Unità organizzativa o persone addette all'adozione
Sistema autenticazione	Accessi non autorizzati	Trattamenti con strumenti elettronici	Sistema integrativo GOOGLE	-	Ufficio ITC
Antivirus	Rischio di intrusione e dell'azione di programmi	Trattamenti con strumenti elettronici	Sentinel One – cyber sicurity	-	Ufficio ITC
Firewall	Protezione degli elaboratori in rete dall'accesso abusivo	Trattamenti con strumenti elettronici	Sentinel One – cyber sicurity	-	Ufficio ITC
Aggiornamenti patch sicurezza	Prevenzione della vulnerabilità degli strumenti elettronici	Trattamenti con strumenti elettronici	Intellope	-	Intellope sro
Gestione supporti rimovibili	Prevenzione trattamenti non autorizzati	Trattamenti con strumenti elettronici	Intellope	-	Intellope sro
Backup/Recovery dati personali	Prevenzione perdita e distruzione dati	Trattamenti con strumenti elettronici	Intellope	-	Intellope sro
Incendio e sicurezza ambientale	Danneggiamento supporti	Tutti i trattamenti	Dispositivi antincendio Sistema ventilazione	-	Responsabile antincendio AQ
Gruppo di continuità	Prevenzione perdita e distruzione dati	Trattamenti con strumenti elettronici	Copertura totale UPS	-	Ufficio ITC New Elettra S.r.l.

ALLEGATI

ALLEGATI A) NOMINE

ALLEGATO A)1
NOMINA A RESPONSABILE PROTEZIONE DEI DATI

ALLEGATO A)2
NOMINA A REFERENTI PRIVACY

ALLEGATO A)3
NOMINA PERSONA AUTORIZZATA AL TRATTAMENTO DATI

ALLEGATO A)4
NOMINA AMMINISTRATORE DI SISTEMA

ALLEGATO A)5
NOMINA AMMINISTRATORE DI SISTEMA ESTERNO

ALLEGATO A)6
NOMINA RESPONSABILE ESTERNO AL TRATTAMENTO DATI

ALLEGATI B) INFORMATIVE

ALLEGATO B)1 - CONSENSO OBBLIGATORIO.
INFORMATIVA SUL TRATTAMENTO DIE DATI PERSONALI DEI DIPENDENTI E DEI COLLABORATORI

ALLEGATO B)2 - CONSENSO OBBLIGATORIO.
INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI DI OPERATORI ECONOMICI (O LORO LEGALI RAPPRESENTANTI) INTERESSATI A PARTECIPARE A PROCEDURA DI SCELTA DEL CONTRAENTE, FORNITORI DI BENI E SERVIZI, FORNITORI DI ATTIVITA' DI QUALSIASI NATURA, COLLABORATORI ESTERNI

ALLEGATO B)3 - CONSENSO OBBLIGATORIO.
INFORMATIVA SUL TRATTAMENTO DIE DATI PERSONALI PER CANDIDATI PROCEDURA SELETTIVA

ALLEGATO B)4 - CONSENSO OBBLIGATORIO/FACOLTATIVO.
INFORMATIVA SUL TRATTAMENTO DIE DATI PERSONALI DEGLI UTENTI DEL PORTALE WEB

ALLEGATO B)5 - CONSENSO OBBLIGATORIO.
INFORMATIVA IN MATERIA DI RIPRESE VIDEOSORVEGLIANZA (CONSENSO ANCHE MINORI)

ALLEGATO B)6 - CONSENSO OBBLIGATORIO
INFORMATIVA RELATIVA ALLE ATTIVITA' DI SORVEGLIANZA SANITARIA E ALLA GESTIONE DELLE CARTELLE SANITARIE A CURA DEL MEDICO COMPETENTE

ALLEGATO B)7 - CONSENSO OBBLIGATORIO
INFORMATIVA PRIVACY USO DEI SOCIAL

ALLEGATO B)8 - CONSENSO OBBLIGATORIO
INFORMATIVA PRIVACY SULLA GESTIONE DELLE SEGNALAZIONI DI "WHISTLEBLOWING

ALLEGATO B)9 - CONSENSO FACOLTATIVO
INFORMATIVA PRIVACY ACCESSO LOCALI

ALLEGATO B)10 - CONSENSO OBBLIGATORIO
INFORMATIVA IN MATERIA DI ACCESSO AREA SAUNA/CENTRO BENESSERE

ALLEGATI C) IMMAGINI

ALLEGATO C)1

AUTORIZZAZIONE ALL'USO DI IMMAGINI FOTOGRAFICHE E VIDEO DIPENDENTI/COLLABORATORI

ALLEGATO C)2

AUTORIZZAZIONE ALL'USO DI IMMAGINI FOTOGRAFICHE E TELEVISIVE, REGISTRAZIONI AUDIO, VIDEO REGISTRAZIONI

ALLEGATO C)3

LETTERA DI AUTORIZZAZIONE AL TRATTAMENTO DIE DATI PERSONALI DIPENDENTI

ALLEGATI D) MODULI

ALLEGATO D)1

SUGGERIMENTI/RECLAMI INFORMATIVA PRIVACY

ALLEGATO D)2

PRESA VISIONE E CONSEGNA DELLA DOCUMENTAZIONE RELATIVA ALLA PRIVACY

ALLEGATO D)3

MODELLO DI COMUNICAZIONE AL GARANTE

ALLEGATI E) VARIE

ALLEGATO E)1

RELAZIONE AI FINI DEL CONTROLLO DELL'OPERATO DEI RESPONSABILI ESTERNI DEL TRATTAMENTO

ALLEGATI F) MINORI

ALLEGATO F)1

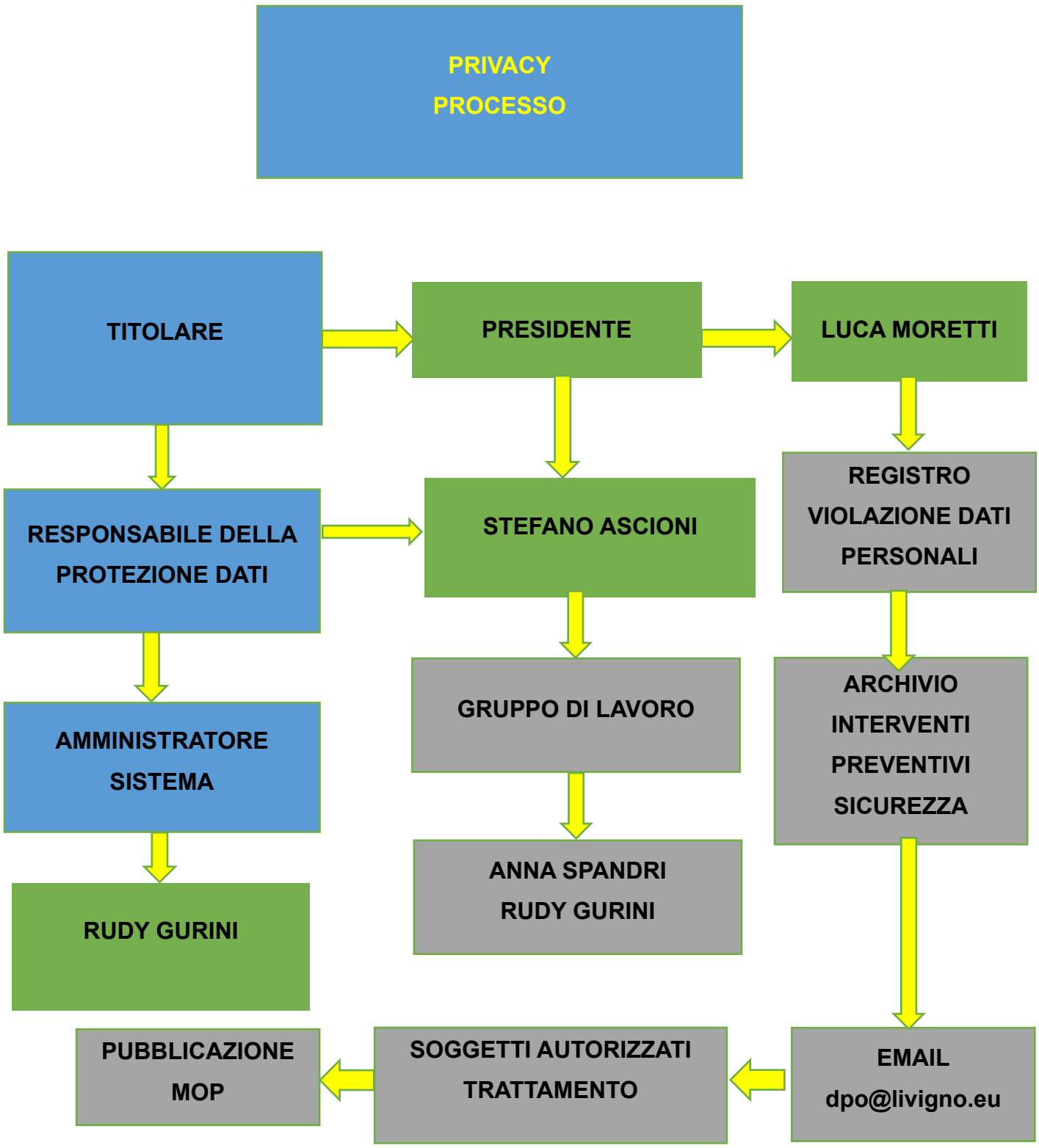
CONSENSO AL TRATTAMENTO DEI DATI PERSONALI DEI MINORI DI ANNI 16

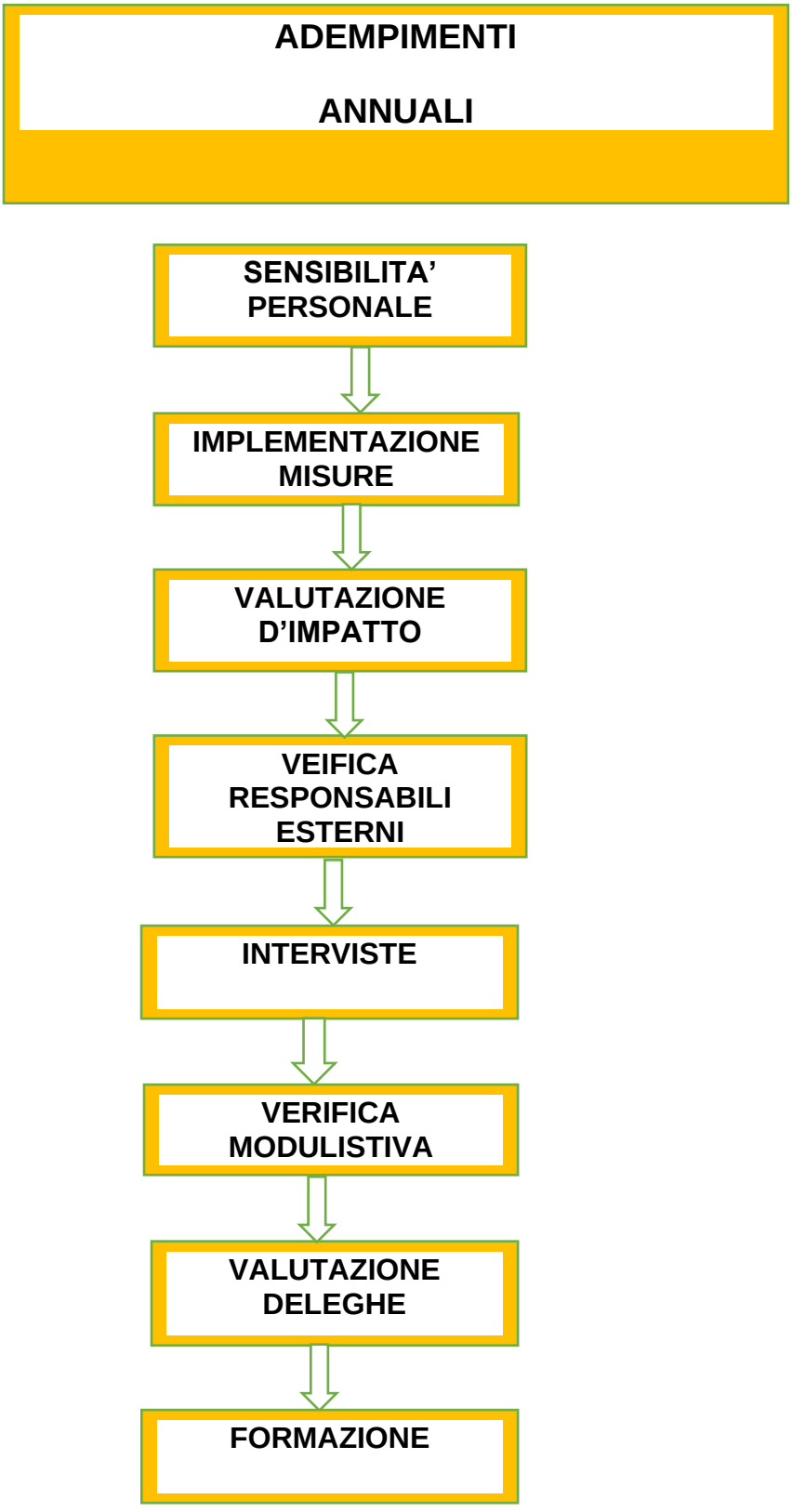
ALLEGATO F)2

LIBERATORIA PER L'UTILIZZO DELLE IMMAGINI DI MINORENNI

ALLEGATO F)3

INFORMATIVA SUL TRATTAMENTO DIE DATI PERSONALI PER MINORI CHE ABBIANO COMPIUTO 16 ANNI


PRIVACY
PROCESSO
TITOLARE
PRESIDENTE
LUCA MORETTI
RESPONSABILE DELLA PROTEZIONE DATI
STEFANO ASCIONI
REGISTRO VIOLAZIONE DATI PERSONALI
AMMINISTRATORE SISTEMA
GRUPPO DI LAVORO
ARCHIVIO INTERVENTI PREVENTIVI SICUREZZA
RUDY GURINI
ANNA SPANDRI
RUDY GURINI
PUBBLICAZIONE MOP
SOGGETTI AUTORIZZATI TRATTAMENTO
EMAIL dpo@livigno.eu


ADEMPIMENTI
ANNUALI
SENSIBILITA' PERSONALE
IMPLEMENTAZIONE MISURE
VALUTAZIONE D'IMPATTO
VEIFICA RESPONSABILI ESTERNI
INTERVISTE
VERIFICA MODULISTIVA
VALUTAZIONE DELEGHE
FORMAZIONE

DICHIARAZIONE DI IMPEGNO E FIRMA

Il presente documento viene firmato in calce da **LUCA MORETTI**, in qualità di Legale Rappresentante.

L'originale del presente documento viene custodito presso la sede della Società, per essere esibito in caso di controlli.

Una copia verrà consegnata a chiunque ne faccia richiesta, in relazione all'instaurarsi di un rapporto che implichi un trattamento congiunto di dati personali (ad esempio, nel caso in cui dovessero essere nominati Responsabili per determinati trattamenti di dati personali).