REGOLAMENTO IN AMBITO PRIVACY

E TRATTAMENTO DEI DATI PERSONALI

REGOLAMENTO COMUNALE IN AMBITO PRIVACY E TRATTAMENTO DEI DATI PERSONALI

Del

COMUNE DI DOVERA

avente sede in Piazza XXV Aprile, 1 - 26010 Dovera (CR)

Anno 2024

Sommario

REGOLAMENTO IN AMBITO PRIVACY E TRATTAMENTO DEI DATI PERSONALI - PREMESSA

Considerando che con il principio introdotto dal nuovo Regolamento Europeo della "responsabilizzazione" (accountability) - che pone in carico al Titolare del trattamento dei dati l'obbligo di attuare politiche adeguate in materia di protezione dei dati, con l'adozione di misure tecniche ed organizzative che siano concretamente e sempre dimostrabili, oltre che conformi alle disposizioni europee (principio della "conformità" o compliance) - vi è l'obbligo di porre in essere comportamenti proattivi, tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento, considerando che ciascun Titolare può scegliere autonomamente il modello organizzativo e gestionale che ritiene più adatto alla propria realtà e dotarsi delle misure di sicurezza che ritiene più efficaci in quanto responsabile delle proprie azioni.

Al fine di garantire all'interno del **Comune di Dovera** avente sede in Piazza XXV Aprile, 1 - 26010 Dovera (CR) (d'ora in avanti "Titolare del Trattamento" o "Ente"), puntuale applicazione della normativa vigente in fatto di protezione di dati personali e del nuovo Regolamento 679/2016 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 e che abroga la direttiva 95/46/CE, si emana il seguente Regolamento in ambito privacy e trattamento dei dati personali, d'ora in avanti Regolamento.

Il suddetto REGOLAMENTO ha come obbiettivo quello di creare un sistema organizzativo efficace e trasparente, che sia immediatamente fruibile e che risponda alle esigenze concrete e quotidiane dei propri operatori.

Il Titolare si impegna a garantire e dimostrare che il trattamento dei dati avviene in maniera conforme a quanto previsto dalla normativa. I dati sono:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per i quali sono trattati;
- esatti e, se necessario, aggiornati; a tal proposito sono state adottate misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per i quali sono trattati;
- trattati in maniera da garantire un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

Il presente documento è aggiornato al

- Regolamento 679/2016 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 e che abroga la direttiva 95/46/CE,
- alle disposizioni legislative di cui al previgente Codice della privacy come modificato al D.lgs. 101 del 10 agosto 2018;
- alla normativa nazionale, anche emanata ai sensi dell'art. 13 della Legge n. 163 del 25 ottobre 2017, e/o dell'Unione Europea rilevante in materia di tutela della riservatezza e dei dati personali;

- ai provvedimenti generali e particolari, le linee guida e le autorizzazioni emanate dall'Autorità Garante per la protezione dei dati personali e/o dal Gruppo dei Garanti Europei della privacy;
- alle disposizioni adottate in relazione allo stato di emergenza epidemiologica da Covid-19 aventi implicazioni in materia di protezione dei dati personali.

Lo stesso può essere di volta in volta integrato in base a diverse disposizioni dettate dai clienti/utenti, dall'entrata in vigore di nuove disposizioni, da implementazioni che l'Ente vorrà apportare.

ENTRATA IN VIGORE DEL REGOLAMENTO E PUBBLICITÀ

Con l'entrata in vigore del presente Regolamento tutte le norme e le disposizioni in precedenza adottate devono intendersi abrogate e sostituite dalle presenti.

Il Regolamento, oltre ad essere affisso nella bacheca Comunale, è pubblicato all'interno del sito web, nella sezione HOME PAGE – Accesso Privacy.

Il presente Regolamento entra in vigore il _____.

TITOLARE DEL TRATTAMENTO

Il Titolare del Trattamento dei dati è **Comune di Dovera.**

Il Titolare del Trattamento, quale responsabile giuridicamente tenuto all'ottemperanza degli obblighi previsti dalla normativa, decide il motivo e le modalità del trattamento e pone in essere misure tecniche e organizzative adeguate per garantire la tutela dei diritti dell'interessato. In ragione delle attività di trattamento svolte, il Titolare del trattamento ha ritenuto necessario designare, ai sensi dell'art. 37 del Regolamento Europeo, un Responsabile della Protezione dei dati o Data Protection Officer che può essere contattato al seguente indirizzo: privacy@comune.dovera.cr.it

Per contattare il Titolare del Trattamento potrà scrivere a **Comune di Dovera** avente sede in Piazza XXV Aprile, 1 - 26010 Dovera (CR) oppure inviare una e-mail all'indirizzo "segreteria@comune.dovera.cr.it oppure tramite pec: dovera@postemailcertificata.it.

PRINCIPI GENERALI IN TEMA DI TRATTAMENTO DEI DATI PERSONALI

I dati sono:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per i quali sono trattati;
- esatti e, se necessario, aggiornati; a tal proposito sono state adottate misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per i quali sono trattati;
- trattati in maniera da garantire un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

FORME DI LEGITTIMAZIONE AL TRATTAMENTO DEI DATI E GESTIONE DEI FLUSSI INFORMATIVI

I dati personali "comuni" (Art. 6 del Regolamento), possono essere trattati se:

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

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

e) il trattamento è necessario per 1'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

I dati "particolari" (Art. 9 del Regolamento), possono essere trattati se:

b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;

h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3;

g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

STRUTTURA DEL REGOLAMENTO

Il presente Regolamento è diviso in sezioni ed è corredata da allegati individuati nello schema che segue, denominati in base alla tipologia di documenti. La procedura contenuta nel Regolamento viene aggiornata ad ogni sostanziale variazione organizzativa e revisionati con periodicità̀ annuale in relazione all'eventuale cambiamento di attrezzature, accorgimenti tecnici o nelle linee guida di tutela.

A CHI E' RIVOLTO	Denominazione
CLIENTI/UTENTI	Informativa generale
DIPENDENTI	Informativa dipendente
DIPENDENTI	Autorizzazione al trattamento dei dati
DIPENDENTI	Autorizzazione al trattamento dei dati – Referente Privacy
AMMINISTRATORI E CONSIGLIERI	Informativa Amministratori e Consiglieri
AMMINISTRATORI E CONSIGLIERI	Autorizzazione al trattamento dei dati Membri del Consiglio
DIPENDENTI/ COLLABORATORI	Assegnazione ed utilizzo dispositivi di sicurezza e dotazione tecnica
DIPENDENTI/ COLLABORATORI	Regolamento in materia di trattamento dei dati personali
FORNITORE / CONSULENTE ESTERNO	Informativa fornitori
FORNITORE / CONSULENTE ESTERNO	Responsabile Esterno del Trattamento
INTERNO	Registro delle Attività di Trattamento come Titolare
INTERNO	Verifica periodica informativa e consenso informato

DEFINIZIONI

(si riportano, per praticità, alcune definizione del Regolamento Europeo)

Ai fini del presente regolamento s'intende per:

«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;

«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;

«limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

«profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

«pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

«archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

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

«responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare e del trattamento;

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

«terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del responsabile;

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

«violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

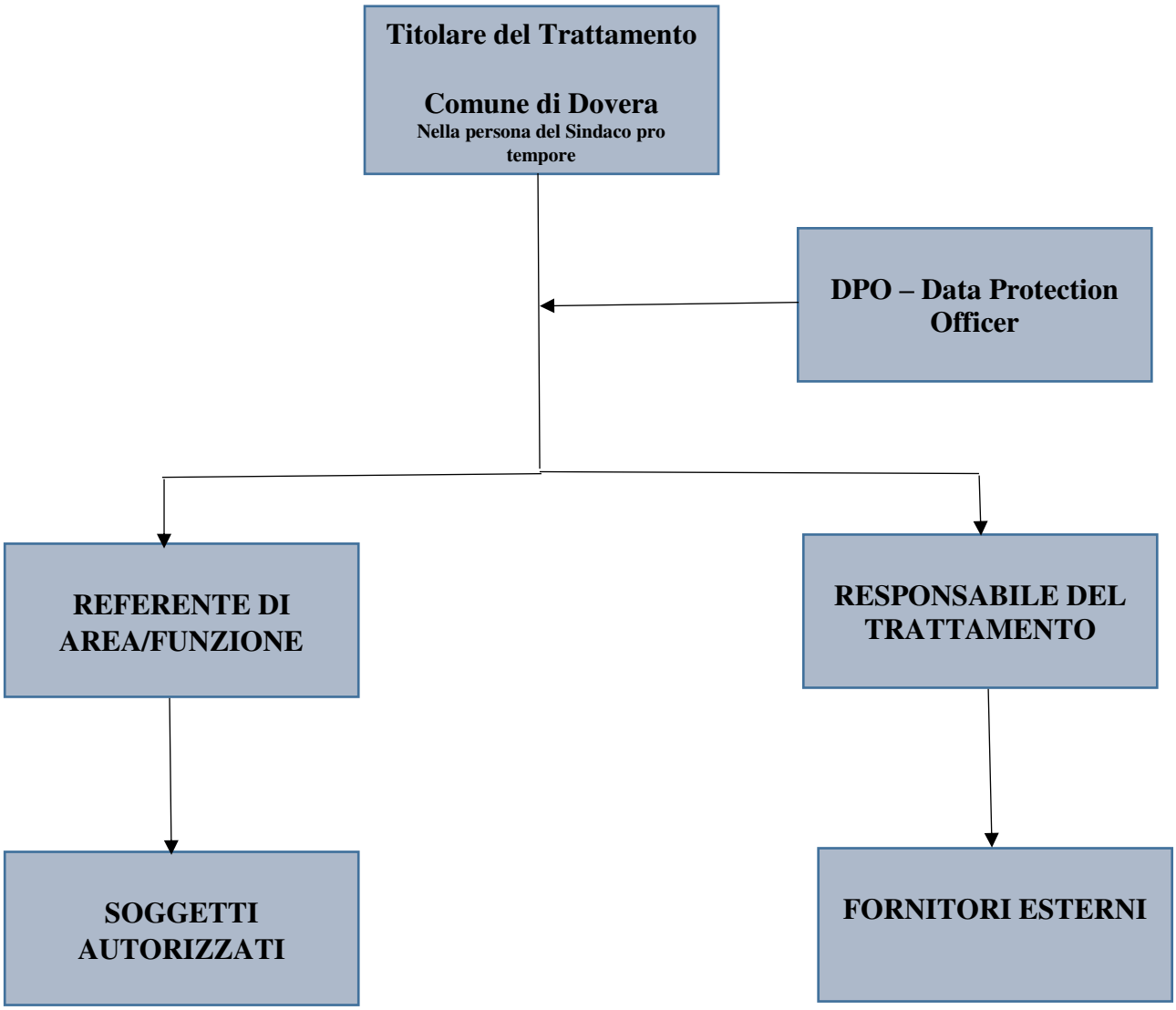
«dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica 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;

«violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati e comunque trattati.

ORGANIGRAMMA IN AMBITO PRIVACY



SENSIBILIZZAZIONE E FORMAZIONE

Il Titolare sostiene e promuove, al suo interno, ogni strumento di sensibilizzazione che possa consolidare il pieno rispetto del diritto alla riservatezza e migliorare la qualità del servizio offerto. A tale riguardo, uno degli strumenti essenziali di sensibilizzazione, anche in materia di privacy, è l'attività formativa del personale e l'attività informativa diretta a tutti coloro che hanno rapporti con la stessa. Per garantire la conoscenza capillare delle disposizioni introdotte dal nuovo Regolamento europeo, e di conseguenza contenute nel presente Regolamento, al momento dell'ingresso in servizio è fornita, a cura della persona preposta, ad ogni dipendente, collaboratore, consulente, ecc. una specifica comunicazione in materia di privacy, con apposita nomina e disposizioni operative e buone prassi, quali "autorizzati al trattamento dei dati" e/o "responsabili al trattamento" ai sensi del Regolamento UE 2016/679.

PERSONE AUTORIZZATE AL TRATTAMENTO DEI DATI PERSONALI SOTTO L'AUTORITÀ DIRETTA DEL TITOLARE

Gli incaricati al trattamento, o persone autorizzate, sono le persone fisiche, dipendenti e collaboratori dell'Ente, incaricati di svolgere le operazioni di trattamento di dati personali di propria competenza con l'indicazione dei compiti e modalità. Le persone autorizzate al trattamento sono individuate dal Titolare del Trattamento, con apposito atto scritto nel quale debbono essere espressamente precisati gli "ambiti" del trattamento consentito (**ALL. Autorizzazione al trattamento dei dati**). A prescindere, comunque, dalla formale attribuzione della qualifica di "incaricato", i dipendenti del Titolare, nonché tutti coloro che vi operano, a qualsiasi titolo, con o senza retribuzione, compresi i tirocinanti e gli stagisti, sono tenuti al rispetto di quanto previsto dal presente Regolamento e dalla normativa vigente, qualora durante la loro attività vengano a conoscenza di dati personali.

Tutti i soggetti di cui sopra, in particolare, sono tenuti a:

- osservare tutte le istruzioni in ordine al trattamento dei dati personali ed ai connessi profili della sicurezza attenendosi alle istruzioni impartite nonché alle specifiche procedure che regolamentino le modalità di utilizzo delle banche dati cui lo stesso abbia accesso;
- astenersi da qualunque comportamento o operazione che non sia coerente con l'espletamento dei propri compiti istituzionali;
- impegnarsi a non comunicare e diffondere all'esterno dell'Ente, per finalità diverse da quelle del rapporto di lavoro, i dati personali di cui siano venuti comunque a conoscenza nell'ambito della propria attività;
- avvisare il Titolare nel caso in cui nello svolgimento di un'attività dovesse riscontrare il trattamento di nuovi dati e finalità o dovesse venir a conoscenza di situazioni che possono essere oggetto di ulteriori valutazioni;
- informare immediatamente il Titolare qualora le istruzioni risultino non conformi alla normativa sulla protezione dai dati o dovesse venire a conoscenza di situazioni non in linea con quanto previsto dalle disposizioni aziendali e che possono comportare rischi per Il Titolare;
- informare il Titolare nell'eventualità di situazioni che possano compromettere la sicurezza informatica in modo che egli sia in grado di adoperarsi in tempo utile ad evitare potenziali rischi.

Le lettere di nomina, firmate per accettazione, e gli elenchi degli incaricati/persone autorizzate sono conservati dal Titolare. Periodicamente, con cadenza almeno annuale, lo stesso procede ad aggiornare la definizione dei dati cui gli incaricati sono autorizzati ad accedere e verifica i requisiti dei trattamenti che sono autorizzati a porre in essere.

RESPONSABILI ESTERNI DEL TRATTAMENTO

Tutti i soggetti esterni che effettuano operazioni di trattamento sui dati dell'Ente, per conto e nell'interesse dello stesso, sono nominati Responsabili Esterni del Trattamento, qualora siano in possesso dei requisiti dalla normativa vigente (esperienza, capacità, affidabilità).

I responsabili esterni hanno l'obbligo di:

- Trattare i dati in modo lecito, secondo correttezza e nel pieno rispetto della normativa vigente in materia di privacy e mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi che gli impone l'articolo 28 del Regolamento e tenere il registro dei trattamenti svolti (ex art. 30, paragrafo 2, GDPR).
- Rispettare le misure di sicurezza previste dal Regolamento e adottare tutte le misure che siano idonee a prevenire ed evitare la comunicazione o diffusione dei dati, il rischio di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non autorizzato o non conforme alle finalità della raccolta;
- Se trattasi di società, nominare al loro interno i soggetti incaricati al trattamento;
- Se trattasi di società, garantire che i dati trattati siano portati a conoscenza soltanto del personale autorizzato;
- Attenersi alle disposizioni impartite dal Titolare del Trattamento;
- La designazione del Responsabile Esterno avviene mediante atto di nomina da parte del Titolare del Trattamento. L'accettazione della nomina e l'impegno a rispettare le disposizioni delle norme vigenti in materia è condizione necessaria per l'instaurarsi del rapporto giuridico tra le parti.

REFERENTE DELLA PRIVACY

Il Titolare del Trattamento ha provveduto a nominare più Referenti Privacy nelle figure dei Responsabili di Settore/Funzione/Area di riferimento (***ALL. Autorizzazione al trattamento dei dati Referente Privacy)*.**

I compiti del Referente privacy, autorizzato con apposito documento, sono

- segnalare al Titolare del Trattamento eventuali richieste ricevute da parte dell'interessato sull'esercizio dei relativi diritti, nonché attenersi alla procedura interna sull'esercizio dei diritti;
- cooperare in caso di attività di controllo in ambito privacy da parte di strutture interne o esterne, fornendo eventuale documentazione richiesta e garantendo l'accesso ai locali;
- informare il Titolare del Trattamento dell'esistenza di un nuovo progetto che impatta sulla protezione dei dati, in applicazione del principio di privacy by design e by default;
- informare il Titolare del Trattamento dell'esistenza di un nuovo trattamento per cui risulta necessario aggiornare il registro o modificarlo, in applicazione del principio di privacy by design e by default;
- informare il Titolare del Trattamento della presenza di una nuova risorsa che tratta dati personali al fine di valutare necessità di formazione in ambito privacy;
- controllare che le persone autorizzate al trattamento rispettino le indicazioni impartite;
- segnalare casi di mancato rispetto delle disposizioni in tema di protezione dei dati al Titolare del Trattamento;
- sorvegliare l'osservanza della normativa in materia di privacy e vigilare sull'effettivo funzionamento delle prescrizioni adottate dall'Ente;

- sorvegliare l'osservanza della normativa in materia di privacy dei Responsabili Esterni del Trattamento e vigilare sull'effettivo funzionamento delle prescrizioni che devono essere adottate dai fornitori;
- aggiornare l'elenco dei fornitori che svolgono funzioni di Responsabili Esterni del Trattamento, a qualsiasi titolo. L'elenco dovrà essere sempre disponibile e messo a disposizione nel caso di richiesta di utenti, interessati e per le autorità di controllo;
- informare i dipendenti che eseguono il trattamento in merito agli obblighi derivanti dalla normativa in materia privacy;
- ricevere e dare esecuzione alle istruzioni e alle prescrizioni impartite dal DPO nominato;
- predisporre e attuare adeguati flussi di comunicazione da e verso il DPO, ivi inclusi gli alert/data breach di sistema;
- fungere da punto di contatto per l'interessato relativamente a tutte le questioni inerenti il trattamento dei loro dati personali e all'esercizio dei diritti.

IMPEGNO ALLA RISERVATEZZA

Il Titolare del Trattamento dei dati si impegna a garantire la riservatezza, conformemente alle procedure interne, e la confidenzialità delle informazioni e dei dati degli interessati acquisiti nel corso della propria attività. A tal scopo, i dati e le informazioni raccolte durante lo svolgimento dell'incarico sono trattati per:

- finalità strettamente connesse alla gestione dell'incarico oggetto del contratto;
- finalità connesse agli obblighi previsti da leggi, regolamenti e normativa comunitaria nonché da disposizioni impartite da autorità a ciò legittimate dalla legge;
- in relazione alle indicate finalità il trattamento dei dati avverrà in modo da garantire la sicurezza e la riservatezza e potrà essere effettuato attraverso strumenti cartacei, informatici e telematici atti a memorizzare, gestire e trasmettere i dati stessi nel rispetto delle misure di sicurezza previste dal Codice.

Tutti i dipendenti e i collaboratori dell'Ente sono tenuti al segreto previsto dall'art. 2105 del codice civile e alla riservatezza dei dati previsto dalla normativa in materia di trattamento dei dati personali. Tutti i dati e le informazioni acquisite potranno essere comunicati esclusivamente a persone e a soggetti terzi espressamente autorizzati a ricevere le informazioni e ad autorità di Vigilanza, italiane o estere, autorità Amministrativa, giudiziaria e fiscale, nei casi e con le limitazioni previste dalla legge, soggetti terzi nell'esecuzione degli obblighi contrattuali assunti nell'ambito di un incarico con il Titolare e dei correlati obblighi di legge, fermo restando che il ricorso a tali soggetti avverrà previo impegno da parte loro a rispettare tutte le prescrizioni in materia di sicurezza dei dati previste dal Codice e dal Regolamento. Il Titolare si impegna a garantire gli standard indicati nelle disposizioni in oggetto nei confronti dei terzi con la medesima diligenza e livello di protezione utilizzati per la sicurezza e la riservatezza dei propri dati.

DATI DEI DIPENDENTI E DEI COLLABORATORI

Il Titolare, al fine di adempiere ai propri obblighi di gestione del personale, raccoglie i dati dei propri collaboratori e dei propri dipendenti, informandoli dei propri diritti. In particolare, il trattamento dei dati delle suddette categorie è previsto per finalità fiscali, amministrative e contabili previste dal contratto, da obblighi di legge e per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento

Altresì è specificato che il Titolare si impegna ad adottare tutte le cautele previste dalla norma e dal Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'Art. 21, comma 1 del d. lgs 10 agosto 2018, n. 101.
Le stesse cautele si applicano ai trattamenti di categorie di dati personali riferiti a candidati all'instaurazione dei rapporti di lavoro, consulenti, agenti, rappresentanti, soggetti che svolgono collaborazioni organizzate dal committente, o altri lavoratori autonomi in rapporto di collaborazione, persone fisiche che ricoprono cariche sociali o altri incarichi nelle persone giuridiche, terzi (familiari e conviventi dei soggetti di cui sopra). Ogni dipendente e collaboratore di cui l'Ente tratta i dati è preventivamente informato sulle modalità e finalità dello stesso prima dell'instaurazione del rapporto (**ALL. Informativa dipendente**).

LA TUTELA DELLA PRIVACY TRA COLLEGHI DI LAVORO

La tutela della privacy è importantissima non solo nella vita privata, ma anche nella vita lavorativa: in questo ambito, il diritto fondamentale alla riservatezza dei lavoratori è sancito da diverse normative.
Fatte queste premesse, è assolutamente vietato acquisire, raccogliere, conservare, archiviare o effettuare qualunque altro tipo di trattamento riguardante i dati personali delle risorse, come colleghi, collaboratori e chiunque altro presti attività lavorativa all'interno dei locali e delle proprietà dell'Ente. Il divieto riguarda ogni tipologia di formato di acquisizione, indistintamente, come documenti cartacei e informatici, fotografie, registrazioni di qualsiasi tipo, accesso alla strumentazione altrui, password e credenziali varie, ecc.

A titolo esemplificativo e non esaustivo, sarà assolutamente vietato:

- accedere al computer di un collega di lavoro senza il suo consenso, anche qualora il dispositivo non richieda di inserire credenziali. Ciò si applica anche quando si conosce la password di accesso di un collega e la si usa per visualizzare dati che non si potrebbero visionare dalla propria postazione;
- leggere le e-mail altrui, in quanto la segretezza della corrispondenza (inclusa la posta elettronica) è tutelata sia dalla Costituzione sia dal codice penale;
- registrare audio e/o video di un collega o scattare fotografie;
- comunicare e/o diffondere informazioni riservate o maldicenze.

Qualunque sia la motivazione, occorre ricordare che questi comportamenti possono avere gravi conseguenze.
Il collega la cui privacy viene violata può infatti presentare una denuncia: in alcuni casi, la lesione della privacy altrui sul posto di lavoro può comportare il licenziamento, mentre in altre situazioni si può rischiare inoltre una pena per il reato di "interferenze illecite nella vita privata" (art. 615 bis del Codice Penale).

DATI DEI CLIENTI/UTENTI

Il Titolare può raccogliere i dati personali dei clienti direttamente presso gli stessi ovvero presso terzi. I dati personali dei clienti/utenti potranno essere trattati nell'ambito della normale attività per le seguenti finalità:

- prestare servizi richiesti e gestire i rapporti con la clientela (es. acquisizione di informazioni preliminari per lo sviluppo e l'esecuzione di un contratto);

- adempiere ad obblighi previsti da un regolamento o dalla normativa comunitaria nonché per osservare disposizioni impartite dalle pubbliche Autorità ed organi di vigilanza e controllo a ciò legittimati dalla legge;
- per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
- per finalità diverse e che richiedono un consenso esplicito e preventivo. Si specifica che è considerato consenso (art. 4, comma 11, GDPR) "qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento").

INFORMAZIONE AGLI INTERESSATI (Informativa)

Il collaboratore/dipendente che per motivi lavorativi si trovi nella condizione di trattare dati personali di terzi, dovrà accertarsi, a ogni nuovo trattamento e preventivamente, che questi abbiano tutte le informazioni relative al trattamento dei dati, con un linguaggio semplice e chiaro, per iscritto o con altri mezzi, anche elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato. In ogni caso è consigliabile consultare il Titolare.
Le informazioni possono essere rilasciate in maniera orale o scritta facendo attenzione a che siano esplicitati alcuni dati, riportati nei paragrafi successivi.

L'informativa (Artt. 13 e 14 del Regolamento) deve essere sempre fornita all'interessato, intesa come persona fisica, prima di effettuare la raccolta dei dati. Se i dati non sono raccolti direttamente presso la persona interessata, l'informativa deve comprendere anche le categorie dei dati personali oggetto di trattamento. In tutti i casi, è obbligo specificare l'identità del Titolare le finalità del trattamento, i diritti degli interessati (compreso il diritto alla portabilità dei dati), e quali sono i destinatari dei dati. Nel caso di dati personali non raccolti direttamente presso l'interessato, l'informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure al momento della comunicazione dei dati (a terzi o all'interessato). L'informativa può anche essere esposta in sintesi purché ci sia una copia integrale della stessa disponibile presso la sede del Titolare del Trattamento e/o nel sito internet.

INFORMAZIONI DA FORNIRE QUALORA I DATI PERSONALI SIANO RACCOLTI PRESSO L'INTERESSATO

In caso di raccolta presso l'interessato di dati che lo riguardano, l'interessato è tenuto a ricevere alcune informazioni tra cui l'identità e i dati di contatto del titolare del trattamento, le finalità e la base giuridica, gli eventuali legittimi interessi perseguiti dal Titolare del Trattamento o da terzi, gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali e, ove applicabile, l'intenzione di trasferire dati personali a un Paese terzo o a un'organizzazione internazionale. In aggiunta alle informazioni di cui sopra, nel momento in cui i dati personali sono ottenuti, l'interessato ha diritto a ricevere informazioni necessarie per garantire un trattamento corretto e trasparente come il periodo di conservazione dei dati personali, i suoi diritti (di cui al paragrafo successivo), l'esistenza di un processo decisionale automatizzato, compresa la profilazione (Art. 22, paragrafi 1 e 4) e informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento è obbligatorio fornire all'interessato informazioni in merito e, se necessario, richiedere preventivamente il consenso.

INFORMAZIONI DA FORNIRE QUALORA I DATI PERSONALI NON SIANO RACCOLTI PRESSO L'INTERESSATO

Qualora i dati non siano stati ottenuti presso l'interessato, lo stesso è tenuto a sapere la fonte da cui hanno origine i dati personali. Le informazioni dovranno essere comunicate entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati. Va inoltre preventivamente specificata la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.

TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI (DATI SENSIBILI)

Come stabilito dall'Art. 9 del Regolamento Europeo 2016/679, è vietato trattare dati personali che rivelino *l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*. Detta disposizione non si applica, secondo il Regolamento UE, quando incorrono alcune condizioni, riportate al summenzionato Art. 9, tra le quali si evidenzia quelle di cui:

- alla lettera "h" ai sensi della quale "il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità (..)";
- alla lettera "b" ai sensi della quale "il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato";
- alla lettera "g" ai sensi della quale "il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato".

Specifiche misure di sicurezza in linea con quanto disciplinato ***all'Art. 32 del Regolamento Europeo*** sono osservate per prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati. Il Titolare effettua un trattamento basato sul principio di Privacy by Design, che richiede che la tutela dei diritti e delle libertà degli interessati con riguardo al trattamento dei dati personali comporti l'attuazione di adeguate misure tecniche e organizzative al momento sia della progettazione che dell'esecuzione del trattamento stesso, onde garantire il rispetto della normativa vigente (art. 25 par. 1 del GDPR). In base al principio della Privacy by Default, il Titolare del Trattamento adotta altresì misure tecniche e organizzative adeguate a garantire il trattamento, per impostazione predefinita, dei soli dati necessari per ogni specifica finalità (art. 25 par. 2 del GDPR).

Si fa presente, inoltre, che il Regolamento UE consente di "mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute" (articolo n. 9, paragrafo n. 4). Posto quanto sopra, si fa rinvio alle vigenti disposizioni emanate, in materia di dati sensibili, biometrici e genetici e in particolare al "Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art.21, comma 1 del D. Lgs 10 Agosto 2018, n. 101" del Garante della Privacy, pubblicato in Gazzetta Ufficiale il 05 Giugno 2019.

TRATTAMENTO DEI DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI (DATI GIUDIZIARI)

Come stabilito dall'Art. 10 del Regolamento Europeo 2016/679, "il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica."
Il Regolamento UE 2016/679 pertanto ravvisa quali condizioni necessarie per il trattamento su detto la presenza di una base giuridica che lo giustifichi (l'art. 6, paragrafo 1 del GDPR) ed altresì il controllo dell'autorità pubblica l'autorizzazione del diritto dell'Unione o degli Stati membri, nel rispetto delle garanzie appropriate per i diritti e le libertà degli interessati. La dottrina prevalente, in merito al fondamento giuridico che consenta di trattare i dati relativi a condanne penali e reati per valutare l'attitudine lavorativa, ha ritenuto che l'autorizzazione da parte del diritto nazionale già risulti presente ai sensi dell'art. 8 del c.d. "Statuto dei Lavoratori" (L. 300/1970) che ne prevede il trattamento nell'ambito della valutazione dell'attitudine lavorativa.

COMUNICAZIONE DI DATI VERSO L'ESTERNO

La comunicazione a soggetti terzi di dati di carattere personale e particolare, detenuti dal Titolare del Trattamento, deve avvenire unicamente in ragione delle finalità per le quali gli stessi sono stati acquisiti e di cui si è data contezza nell'informativa privacy consegnata e sottoscritta dagli interessati.
La diffusione di dati che ecceda quanto su indicato, deve considerarsi illecita. L'eventuale comunicazione di dati particolari e giudiziari tra soggetti pubblici, è ammessa solo in presenza di una normativa o di un regolamento che la giustifichino e, in ogni caso, qualora risulti necessaria per lo svolgimento di funzioni istituzionali, anche a seguito di un bilanciamento degli interessi.

UTILIZZO DI VIDEO E FOTOGRAFIE

La pubblicazione di una fotografia su qualunque tipo di supporto, informatico e non, che comunque arriva a un numero di utenti non definiti, non solo si inquadra nel trattamento di dati personali e sensibili, e costituisce interferenza nella vita privata di una persona, ma alla luce nel nuovo Regolamento Europeo è definita DIFFUSIONE, ovvero dare conoscenza dei dati a soggetti indeterminati, in qualunque forma anche mediante la loro messa a disposizione o consultazione. Si ha, quindi, una diffusione anche quando si pubblica online, ad esempio una fotografia su un social network. In assenza di consenso tale attività è da ritenersi illecita.

Premesso che

- l'articolo 96 della legge 633/1941 sul diritto d'autore stabilisce che "Il ritratto di una persona non può essere esposto, riprodotto o messo in commercio senza il consenso di questa";
- l'articolo 10 del Codice Civile (Abuso dell'immagine altrui) stabilisce che "Qualora l'immagine di una persona o dei genitori, del coniuge o dei figli sia stata esposta o pubblicata fuori dei casi in cui l'esposizione o la pubblicazione è dalla legge consentita, ovvero con pregiudizio al decoro o alla reputazione della persona stessa o dei detti congiunti, l'autorità giudiziaria, su richiesta dell'interessato, può disporre che cessi l'abuso, salvo il risarcimento dei danni";
- l'articolo 2043 del Codice Civile (Risarcimento per fatto illecito) stabilisce che "Qualunque fatto doloso o colposo, che cagiona ad altri un danno ingiusto, obbliga colui che ha commesso il fatto a risarcire il danno".

È fatto divieto fare, conservare, comunicare immagini e video, audio con oggetto l'Ente, i clienti e i dipendenti e collaboratori dello stesso.

DIRITTI DELL'INTERESSATO

Uno degli obiettivi principali del Regolamento Europeo consiste nel garantire la privacy e la protezione dei dati personali degli interessati. Per aiutare gli interessati a garantire la protezione e la riservatezza dei propri dati personali, il Regolamento Europeo conferisce ai soggetti interessati determinati diritti attraverso i quali presentare una richiesta specifica e assicurarsi che i propri dati personali non vengano utilizzati in modo improprio per finalità diverse dallo scopo legittimo per il quale sono stati originariamente forniti.

Il Titolare del Trattamento agevola l'esercizio dei diritti dell'interessato ai sensi degli articoli da 15 a 22, senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste.

Diritto di accesso dell'interessato (Art. 15)

L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

le finalità del trattamento;

le categorie di dati personali in questione;

i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;

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

l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;

il diritto di proporre reclamo a un'autorità di controllo;

qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;

l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

2. Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.

3. Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

4. Il diritto di ottenere una copia di cui al paragrafo 3 non deve ledere i diritti e le libertà altrui.

Diritto di rettifica (Art. 16)

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Diritto alla cancellazione («diritto all'oblio») (Art. 17)

L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;

l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;

i dati personali sono stati trattati illecitamente;

i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;

i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.

2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:

per l'esercizio del diritto alla libertà di espressione e di informazione;

per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;

a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o

per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Diritto di limitazione di trattamento (Art. 18)

L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:

l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;

il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;

benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;

l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

2. Se il trattamento è limitato a norma del paragrafo 1, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

3. L'interessato che ha ottenuto la limitazione del trattamento a norma del paragrafo 1 è informato dal titolare del trattamento prima che detta limitazione sia revocata.

Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento (Art. 19)

Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma dell'articolo 16, dell'articolo 17, paragrafo 1, e dell'articolo 18, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

Diritto alla portabilità dei dati (Art. 20)

L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:

il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e

il trattamento sia effettuato con mezzi automatizzati.

2. Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.

3. L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

4. Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui.

Sezione 4

Diritto di opposizione e processo decisionale automatizzato relativo alle persone fisiche

Diritto di opposizione (Art. 21)

L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.

Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità.

Il diritto di cui ai paragrafi 1 e 2 è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.

Nel contesto dell'utilizzo di servizi della Società dell'informazione e fatta salva la direttiva 2002/58/CE, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.

Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione (Art. 22)

L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

Il paragrafo 1 non si applica nel caso in cui la decisione:

sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;

sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;

si basi sul consenso esplicito dell'interessato.

Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.

Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

Comunicazione di una violazione dei dati personali all'interessato (Art. 34)

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).

Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:

il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle

destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

ESERCIZIO DEI DIRITTI DELL'INTERESSATO

La richiesta per l'esercizio dei diritti può essere fatta pervenire:
tramite mail all'indirizzo Pec: dovera@postemailcertificata.it o tramite raccomandata a **Comune di Dovera** avente sede in Piazza XXV Aprile, 1 - 26010 Dovera (CR) specificando il motivo della stessa:

- direttamente dall'interessato con l'esibizione di un documento di riconoscimento o allegandone copia o anche con altre adeguate modalità o in presenza di circostanze atte a dimostrare l'identità personale dell'interessato stesso;
- tramite altra persona fisica o associazione, a cui abbia conferito per iscritto delega o procura; in tal caso la persona che agisce su incarico dell'interessato deve consegnare copia della procura o della delega, nonché copia fotostatica non autentica di un documento di riconoscimento del sottoscrittore;
- in caso di persone decedute, tali diritti possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni famigliari meritevoli di protezione;
- se l'interessato è una persona giuridica, la richiesta è avanzata dalla persona fisica legittimata.

La richiesta per l'esercizio dei diritti può essere esercitata dall'interessato solo in riferimento alle informazioni che lo riguardano e non anche ai dati relativi ai terzi, eventualmente presenti all'interno dei documenti che lo riguardano.
Il soggetto competente alla valutazione dell'istanza è il Titolare del Trattamento nella figura del legale rappresentante. All'istanza deve essere dato riscontro entro 30 giorni dalla data di ricezione della stessa. I termini possono essere prolungati di altri 60 giorni previa tempestiva comunicazione all'interessato, qualora l'istanza avanzata dal richiedente sia di particolare complessità o ricorra un giustificato motivo.

COMUNICAZIONE DI UNA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

(Art. 33/34 del Regolamento Europeo)

Con il Data Breach, o violazione di dati personali, è una violazione di sicurezza che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.
Alcuni possibili esempi:
- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;

- la divulgazione non autorizzata dei dati personali.

In caso di violazione di dati personali il Titolare senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, deve notificare la violazione al Garante per la protezione dei dati personali a meno che sia improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche. A partire dal 1° luglio 2021, la notifica di una violazione di dati personali deve essere inviata al Garante tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/

Inoltre, se la violazione comporta un rischio elevato per i diritti delle persone, il titolare deve comunicarla a tutti gli interessati, utilizzando i canali più idonei, a meno che abbia già preso misure tali da ridurne l'impatto. Il titolare, a prescindere dalla notifica al Garante, documenta tutte le violazioni dei dati personali, ad esempio predisponendo un apposito registro. Tale documentazione consente all'Autorità di effettuare eventuali verifiche sul rispetto della normativa.

Per consentire al Titolare di far fronte ai suoi obblighi verso gli interessati, ognuno che abbia il sospetto di un avvenuto data breach o di un possibile avvenimento similare, come eventuali violazioni dei dati o incidenti informatici, che possa mettere a rischio la sicurezza dei dati contenuti nelle banche dati del Titolare, deve immediatamente comunicarlo in modo da poter mettere in atto, in maniera puntuale e tempestiva, la procedura di riferimento.

CHE TIPO DI VIOLAZIONI DI DATI PERSONALI VANNO NOTIFICATE?

Vanno notificate unicamente le violazioni di dati personali che possono avere effetti avversi significativi sugli individui, causando danni fisici, materiali o immateriali. Ciò può includere, ad esempio, la perdita del controllo sui propri dati personali, la limitazione di alcuni diritti, la discriminazione, il furto d'identità o il rischio di frode, la perdita di riservatezza dei dati personali protetti dal segreto professionale, una perdita finanziaria, un danno alla reputazione e qualsiasi altro significativo svantaggio economico o sociale.

REGISTRAZIONE DEL DATA BREACH

È comunque sempre necessario documentare qualsiasi violazione (Registro Data Breach), sia che non presenta un rischio per i diritti e le libertà delle persone sia che presenta un rischio per i diritti e le libertà delle persone: in sostanza che bisogna essere accountable, dimostrare accountability. Tale documentazione consente all'Autorità di effettuare eventuali verifiche sul rispetto della normativa e permette al titolare del trattamento di registrare i dettagli relativi alla violazione, comprese le cause, i fatti e i dati personali interessati in modo da poter valutare i provvedimenti per porvi rimedio.

DISPOSIZIONI GENERALI

Il Titolare mette in atto misure di sicurezza tali da garantire l'integrità, la disponibilità e la riservatezza dei dati trattati, sia in termini di allocazione delle risorse umane e delle risorse tecnologiche, sia in termini normativi e comportamentali in funzione di una maggior "responsabilizzazione" (accountability) nei confronti della materia.

La stessa, ponendo grande attenzione agli aspetti della sicurezza individua, definisce e assegna formalmente i ruoli e le responsabilità inerenti il trattamento delle informazioni e dei dati. Il Titolare ricorda che nell'esecuzione delle proprie mansioni l'incaricato potrà venire a conoscenza di informazioni riservate, sia di tipo commerciale/finanziario, che di dati personali riferibili a terzi. I dati suddetti, oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite, in base al progresso tecnico, alla natura dei dati ed alle specifiche caratteristiche del trattamento, in modo tale da ridurre al minimo, mediante l'adozione di idonee misure di sicurezza, i rischi di distribuzione o di perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito e non conforme alle finalità di raccolta.

Il trattamento è limitato a quei dati strettamente necessari mentre rimangono vietate operazioni e trattamenti di qualunque genere che vadano oltre le proprie mansioni. La comunicazione è proibita, se non quella effettuata per finalità lavorative alle parti terze individuate su richiesta di forze di polizia, autorità giudiziaria, organismi di informazione e sicurezza o da altri soggetti pubblici, per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.

MISURE DI SICUREZZA

La responsabilità dell'attività di impostazione e coordinamento dei sistemi che garantiscono la sicurezza e la tutela di tutti i dati oggetto di trattamento sia da un punto di vista logico che fisico, la loro gestione diretta o tramite fornitori, sono in carico del Responsabile Esterno della Sicurezza Informatica. La responsabilità dell'attività di coordinamento delle attività e delle procedure organizzative della privacy sono a carico del Titolare.

In base alle figure professionali presenti in azienda, vengono definiti i profili standard da assegnare agli utenti con le autorizzazioni necessarie all'espletamento delle rispettive mansioni definite per ruoli e competenze. La validità delle richieste di accesso alla rete è verificata automaticamente dal sistema stesso prima di consentire l'accesso ai dati, tramite un sistema di autenticazione e autorizzazione impostate di default (Privacy by Default).

Per garantire l'integrità a protezione dell'accesso ai dati sono adottate misure di sicurezza volte a minimizzare i rischi che le informazioni siano rivelate o modificate senza autorizzazione, ovvero perse o alterate accidentalmente o intenzionalmente. Il sistema in atto prevede un

- sistema di autenticazione per assicurare che la persona che accede al sistema sia identificata con certezza;
- sistema di autorizzazione che prevede che a ciascuna persona che accede al sistema sia assegnato un profilo di accesso che definisce i dati ai quali l'utente è autorizzato ad accedere e, ove applicabile, le operazioni che per ciascun dato o gruppo di dati è autorizzato ad eseguire (consultazione, inserimento, modifica, cancellazione, ecc).

Ogni dispositivo utilizzato dall'utente è censito dal Titolare. Per ridurre il rischio di violazioni della sicurezza della postazione di lavoro, per prevenire eventi di data breach e responsabilizzare i dipendenti aziendali, si richiede il rispetto delle seguenti buone prassi:

- garantire che tutte le informazioni sensibili o confidenziali in formato elettronico o cartaceo siano messe al sicuro nella propria postazione di lavoro, in particolare alla fine della giornata lavorativa e in caso di assenza prolungata;
- rendere il pc non utilizzabile quando ci si allontana dalla postazione di lavoro, attivando lo screen saver disattivabile tramite password;
- spegnere i pc alla fine della giornata lavorativa;
- rimuovere qualsiasi informazione e/o dato particolare/sensibile dalla scrivania e chiuderla a chiave in un cassetto quando la postazione di lavoro non è occupata e alla fine della giornata lavorativa;
- non lasciare incustoditi i dispositivi (laptop, smartphone o tablet, chiavette USB, ecc) soprattutto se contenenti le informazioni riservate e/o dati particolari/sensibili;
- non lasciare incustodite le password su note adesive e in modalità che siano accessibili a terzi;
- rimuovere dalle stampanti stampe contenenti informazioni riservate e/o dati particolari/sensibili;
- distruggere tramite distruggidocumenti i documenti riservati o contenenti dati particolari/sensibili al momento del loro smaltimento.

Il dipendente che viola queste norme di comportamento e che causa "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, comma 1, n. 12 del Regolamento UE n. 2016/679), accidentalmente (ad esempio per mero errore) oppure illecitamente, ossia per mezzo di una azione deliberata, può essere soggetto ad azioni disciplinari.

ACCESSO AI LOCALI

Con riferimento ai locali aziendali la responsabilità della conservazione e sicurezza dei medesimi spetta al Titolare del Trattamento. L'accesso agli stessi è autorizzato solo per finalità lavorative e attraverso le modalità impartite (**ALL: Assegnazione ed utilizzo dispositivi di sicurezza e dotazione tecnica**). Non sono ammesse persone estranee. È obbligo chiudere la porta dei locali ogni qualvolta si esce. Dovrà essere cura della persona mantenere in modo ordinato e senza materiali superflui o infiammabili l'intera area utilizzata per l'espletamento delle proprie mansioni.

TRATTAMENTO DEI DATI SENZA L'AUSILIO DI SUPPORTI ELETTRONICI

La documentazione cartacea, soprattutto contenente dati particolari e/o rilevanti per il Titolare e per i clienti/utenti dello stesso, è sempre archiviata all'interno di cartelline non trasparenti e riposta all'interno di mobili chiusi a chiave. Allo stesso modo i documenti e/o supporti contenenti note od appunti relativi a pratiche in corso sono conservati chiusi e fuori dalla portata di estranei.

È opportuno prelevare di volta in volta solo il materiale strettamente necessario all'operazione, e riporlo poi a posto al termine delle operazioni di trattamento. Al fine di cautelarsi rispetto al rischio di accessi non autorizzati a dati e documenti occorre garantire sempre la massima attenzione nella gestione delle informazioni, ponendo sempre cura nel minimizzare i supporti in cui vengono riportate e garantendo la protezione di questi.

Appunti, informazioni, note, non vanno trascritti in supporti che possono essere visti, smarriti e/o che non garantiscono idonea sicurezza. Premettendo che è buona prassi limitare il numero di fotocopie dei documenti trattati, non è consentito in alcun caso utilizzare carta riciclata per la stampa o per gli appunti. La carta da gettare è distrutta tramite distruggi

documenti che è posizionata all'interno dei locali. La carta che non contiene informazioni di cui sopra, come dispense di studio, pubblicità, ecc …, viene gettata nel raccoglitore per la raccolta differenziata adibito.
Quando i documenti devono essere trasportati all'esterno del luogo di lavoro, l'incaricato deve sempre tenere con sé una cartella in cui custodirli, adottando le misure necessarie ad evitare che sia possibile visionare il contenuto della stessa. La cartella non dovrà mai essere lasciata incustodita.
Nel caso si rende necessario la consultazione, l'archiviazione di informazioni personali e/o di documenti, come possono essere anche quelli di riconoscimento, che contengano dati personali, l'incaricato, che deve avere i requisiti per poter visionare gli stessi, dovrà archiviarli con cura nel reparto/archivio di riferimento prestabilito dal Titolare del Trattamento. Si dovrà in questo caso aver cura di riferire all'interessato le modalità di trattamento che verrà fatto dei dati, chiedendo allo stesso se necessita dell'informativa del Titolare.

ARCHIVI CARTACEI

In considerazione dell'attività svolta, il patrimonio documentale dell'Ente è una risorsa di primaria importanza, per tale motivo gli archivi cartacei hanno bisogno delle migliori misure di sicurezza per garantire la conservazione di informazioni fondamentali alla continuità operativa, e della memoria storica dell'Ente. Un archivio cartaceo può rappresentare una vera e propria minaccia all'incolumità degli addetti, delle strutture e dell'ambiente circostante, ove non fossero adottate le norme di sicurezza adeguate a un deposito cartaceo.
I locali adibiti a depositi di materiale cartaceo devono avere determinate caratteristiche a seconda dell'entità dell'archivio e del numero dei lavoratori impiegati (accessibilità, eventuali porte taglia-fuoco, ventilazione e filtri a prova di fumo, scaffalature, impianti elettrici, impianti di rilevazione ed estinzione incendi, etc.).
Per questi motivi, considerando la funzione pubblica svolta dall'Ente, agli archivi potrà accedere esclusivamente personale autorizzato.
Inoltre una sede di conservazione archivistica deve innanzitutto essere collocata in un'area priva di rischi. Sono pertanto da evitare collocazioni insistenti o prossime ad aree di esondazione, fiumi, torrenti, canali, frane. Ugualmente da evitare sono collocazioni prossime a sedi industriali o manifatturiere potenzialmente pericolose (centrali elettriche, raffinerie, industrie chimiche) o a magazzini e depositi in cui sia conservato materiale pericoloso (autorimesse, depositi di detersivi e sostanze infiammabili, depositi di materiale plastico ecc.).
Alcuni locali, quali le cantine, i locali interrati o i sottotetti sono inadatti per loro stessa natura, poiché inevitabilmente esposti a rischi di allagamento o a instabili condizioni di umidità e temperatura, con grandi variazioni stagionali. Nei casi in cui sia assolutamente impossibile rinunciare a questi tipi di locale quali sedi di conservazione, sarà allora necessario adottare tutte le precauzioni e gli accorgimenti strutturali necessari a scongiurare i relativi rischi. È di fondamentale importanza adottare tutte le misure di sicurezza preventive e necessarie al fine di minimizzare al massimo i rischi di distruzione del materiale cartaceo, ad esempio prestando la massima attenzione a non riporre all'interno degli archivi materiali e/o sostanze pericolosi e/o infiammabili, nonché adottare tutte le misure comportamentali orientate a tal fine (ad esempio non fumare, non accedere con sostanze liquide, soprattutto se infiammabili e se fossero presenti cavi, quadri elettrici e interruttori vari).

COMUNICAZIONE DI DATI PERSONALI

Rimane buona norma evitare di raccogliere e/o comunicare dati personali per telefono, se non si è certi che il corrispondente sia una persona autorizzata a trattare determinati dati. Valgono per le comunicazioni orali, telefoniche

e di persona, le stesse attenzioni utilizzate per la protezione dei dati in forma scritta.
Inoltre per la comunicazione di dati a soggetti terzi o con strumenti impersonali o che non consentono un controllo effettivo dell'identificazione del chiamante, è opportuno controllare l'identità del richiedente eventualmente ponendo dei quesiti e nell'accogliere la richiesta è opportuno fare attenzione all'esattezza del dato che viene comunicato, soprattutto quando la richiesta viene soddisfatta telefonicamente o attraverso trascrizione da parte dell'operatore di quanto visualizzato sul monitor.

TRATTAMENTO DI INFORMAZIONI RISERVATE/ DATI PARTICOLARI

Anche se trattasi di ipotesi remota, colui che viene a contatto con informazioni riservate e/o dati particolari e giudiziari che non siano di sua diretta competenza, deve assicurare le stesse da in modo che non siano visibili a terzi e procedere alla comunicazione al Titolare del Trattamento.

SMALTIMENTO DEI DOCUMENTI CONTENENTI DATI E INFORMAZIONI

In ottemperanza alle disposizioni in materia di trattamento di dati personali, i documenti cartacei da cestinare, soprattutto nel caso contengano dati personali e sensibili, ma anche informazioni aziendali riservate, devono essere prima distrutti con il distruggidocumenti.

UTILIZZO DEGLI STRUMENTI INFORMATICI

SISTEMA ELETTRICO E SISTEMA INFORMATICO

L'accesso al sistema da parte dei dipendenti, collaboratori, o chiunque per finalità esplicite e precise si trovi a utilizzarlo, dovrà avvenire in conformità a quanto previsto dal presente regolamento e/o in conformità al regolamento alla quale il sistema fa riferimento. Si precisa che l'accesso e l'utilizzo sono consentiti ai soli fini dell'esecuzione della prestazione per la quale l'utente è stato abilitato, come previsto da autorizzazione rilasciata dal Titolare (ALL. Autorizzazione al trattamento dei dati).
La rete internet è uno strumento di lavoro. È per questo vietato compiere attività che appesantiscano il traffico o i servizi sulla rete, come pure compiere attività che possano causare disturbi al sistema senza valutarne adeguatamente le conseguenze.

Al fine di salvaguardare il corretto funzionamento della rete elettrica e della rete internet e tutte le impostazioni a esse connesse, si fa presente che non è consentito:

- accedere a linee informatiche non consentite e non specificate nelle proprie lettere di incarico e /o accedere a linee non conosciute con gli strumenti di lavoro;
- accedere ai quadri elettrici e/o modem, ne modificare alcun settaggio dell'impiantistica installata nell'area di lavoro;
- utilizzare apparecchiature che possano causare particolari picchi o abbassamenti di tensione o compiere attività che possano creare particolari rischi di incendio od esalazioni tossiche;

- utilizzare cavi, prolunghe, connettori, etc, non certificate alle norme vigenti e non autorizzate dall'Azienda;
- eseguire installazioni, alterazioni (inclusa installazione di software di qualsiasi genere, licenziato e non licenziato) e modifiche, dismissioni di materiale e/o componenti hardware e software, e supporti di memorizzazione di qualsiasi tipo;
- installare infrastrutture di networking, comunicazione o connettività, di tipo locale o remoto, fatto salvo esigenze derivanti da obblighi contrattuali preventivamente ed esplicitamente previste;
- utilizzare di strumenti preposti alla scansione ed alla rilevazione delle vulnerabilità di sistemi, applicazioni e servizi, così come di soluzioni hardware e software identificate, considerate o riconosciute come strumenti di hacking, cracking o diffusione di virus e spam;
- utilizzare dispositivi e apparati di trattamento dei dati quali ad esempio PC, work station, dispositivi di memorizzazione, etc, che non siano autorizzati dal Titolare o che, anche se autorizzati, non rispondano ai requisiti di sicurezza stabiliti dalla legislazione in merito;
- scaricare software gratuiti, se non espressamente autorizzati;
- partecipare a forum non professionali, chat line.

Si ricorda, inoltre, che la navigazione in Internet non è assolutamente anonima e la semplice visualizzazione di una pagina web comporta l'inserimento automatico in una certa serie di log files mantenuti dalle varie macchine. Si tratta di log automatici, che sono raccolti solo per eventuali problemi di ordine giudiziario; infatti, nel caso di attività illegali svolte su Internet, la Polizia Postale e delle Telecomunicazioni può richiedere l'accesso ai file di log dei vari provider e verificare da quale connessione Internet è stato generato il traffico, risalendo, quindi, sino all'Ente che è il Titolare del trattamento.

PROTEZIONE ANTIVIRUS

Ogni incaricato del trattamento deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software aggressivo (ad es. lo spyware).
I dispositivi in uso presso l'Ente sono dotati di sistema antivirus automatici. Ogni incaricato del trattamento è comunque invitato a controllare dalla propria postazione lavorativa tutti i file provenienti dall'esterno, secondo le istruzioni ricevute e ad adottare diligentemente le opportune cautele al momento della trasmissione di file all'esterno. Inoltre è altresì obbligo controllare il regolare funzionamento e l'aggiornamento periodico del software antivirus installato e nel caso che il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso, senza spegnere il computer e dovrà segnalare l'accaduto al Responsabile dell'infrastrutture informatiche.

CONSERVAZIONE/ARCHIVIAZIONE

La documentazione acquisita in formato elettronico è conservata all'interno del server comunale.
Non è consentito salvare informazioni aziendali sui propri dispositivi personali. Nel caso sia necessario conservare la documentazione nel proprio dispositivo per lo svolgimento di attività lavorative, questa dovrà essere conservata solo per il tempo necessario allo svolgimento delle stesse. Sarà cura dell'utente, e sotto la propria responsabilità, gestire i requisiti idonei di sicurezza del dispositivo per mantenere le condizioni di integrità e riservatezza dei dati, soprattutto nel caso di utilizzo di un dispositivo portatile fuori dai locali del Titolare. Non è consentito utilizzare i server aziendali per la conservazione di documentazione personale e non inerente l'attività lavorativa.

GESTIONE DELLE PASSWORD

La rete, i PC e i dispositivi dati in uso al dipendente sono protetti da password e, dove necessario, da accesso autorizzato tramite credenziali, previste ed attribuite dal Titolare del Trattamento.

La password sono obbligatorie per l'accesso al computer, alla rete e ai dispositivi di lavoro. Le stesse sono strettamente personali. Le password sono segrete e vanno comunicate, ad ogni cambio, al Titolare del Trattamento, che provvederà a conservarle in un luogo non accessibile. Le password non saranno utilizzate se non in caso di assoluta necessità per garantire la continuità lavorativa, in caso di richiesta da Forze dell'Ordine e/o giudiziarie, o/e comunque previa comunicazione all'interessato.

Le password devono essere modificate a cura dell'incaricato del trattamento al primo utilizzo e ogni 6 mesi (3 mesi in caso di trattamento dei dati personali).

Il Garante Privacy ha fornito dei suggerimenti per scegliere le proprie password e conservarle in modo sicuro.

Una buona password:

- deve essere abbastanza lunga: almeno 8 caratteri, anche se più aumenta il numero dei caratteri più la password diventa "robusta" (si suggerisce intorno ai 15 caratteri);
- deve contenere caratteri di almeno 4 diverse tipologie, da scegliere tra: lettere maiuscole, lettere minuscole, numeri, caratteri speciali (cioè punti, trattino, underscore, ecc.);
- non deve contenere riferimenti personali facili da indovinare (nome, cognome, data di nascita, ecc.). Non deve nemmeno contenere riferimenti al nome utente (detto anche user account, alias, user id, user name);
- meglio evitare che contenga parole "da dizionario", cioè parole intere di uso comune: è meglio usare parole di fantasia oppure parole "camuffate" per renderle meno comuni, magari interrompendole con caratteri speciali (ad esempio: caffè può diventare caf-f3). Esistono infatti software programmati per tentare di indovinare e rubare le password provando sistematicamente tutte le parole di uso comune nelle varie lingue, e con questa accortezza si può rendere il loro funzionamento più complicato;
- andrebbe periodicamente cambiata, soprattutto per i profili più importanti o quelli che usi più spesso (e-mail, e-banking, social network, ecc.);
- utilizza password diverse per account diversi (e-mail, social network, servizi digitali di varia natura, ecc.). In caso di «furto» di una password si evita così il rischio che anche gli altri profili che ti appartengono possano essere facilmente violati.
- altra accortezza importante è quella di NON utilizzare password già utilizzate in passato.
- occorre poi ricordare che le eventuali password temporanee rilasciate da un sistema o da un servizio informatico vanno sempre immediatamente cambiate, scegliendone una personale.

È fatto divieto memorizzare nel dispositivo credenziali, parole chiavi e password private. È obbligo dell'incaricato che ha in uso il dispositivo provvedere alla pulizia dei dati e delle password che rimanessero memorizzati nel dispositivo.

La Password deve essere sostituita:

- ad ogni dimenticanza della stessa da parte dell'incaricato, previa operazione di sblocco da parte del Titolare del Trattamento;
- ogni sei mesi/ tre mesi o al primo accesso successivo a tale scadenza;
- al primo accesso successivo ad un accesso di terzi autorizzato dal Titolare del Trattamento.

L'incaricato è consapevole che le operazioni effettuate attraverso l'utilizzo delle password e di credenziali ricadono direttamente sotto la responsabilità del soggetto. È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato.

CASELLA DI POSTA ELETTRONICA

All'interno dell'Ente possono esserci indirizzo e-mail personali abbinati al singolo lavoratore dipendente (nomecognome@nomeazienda.it) o condivisi in base all'area di riferimento.

Premettendo che la "personalizzazione" dell'indirizzo non comporta la sua "privatezza", in quanto trattasi di strumenti di esclusiva proprietà comunale, si specifica che la mail è messa a disposizione del dipendente al solo fine dello svolgimento delle proprie mansioni lavorative.

A tal fine ogni utente sarà responsabile del corretto utilizzo della stessa.

A tal fine si precisa che:

- tutti i messaggi in entrata e in uscita dagli indirizzi di posta elettronica comunale sono di proprietà dell'Ente;
- il messaggio di posta elettronica comunale, sia individuale che condiviso si configura come corrispondenza aperta che potrebbe essere letto da chiunque durante il suo percorso sulla rete internet fino al destinatario nonché dagli addetti IT sul server comunale che gestisce il servizio stesso;
- l'uso degli indirizzi di posta elettronica comunali è ammesso esclusivamente per motivi attinenti all'attività lavorativa. È fatto divieto di utilizzare le caselle di posta elettronica comunale per l'invio di messaggi personali o per altra funzione diversa da quella esplicitamente autorizzata. Sulla base di ciò nessuna aspettativa di tutela del proprio diritto alla privacy, relativa ai messaggi di posta elettronica in entrata ed in uscita utilizzando l'indirizzo comunale, potrà essere pretesa dal suo utilizzatore;
- le informazioni aziendali trattate attraverso la posta elettronica vanno inviate solo a mail ufficiali e/o aziendali. Non possono essere inviate a indirizzi personali e non ufficiali, anche se appartenenti al medesimo destinatario. È fatto divieto inviare a indirizzi di posta elettronica privata e-mail con allegati documenti aziendali o, anche senza allegati, e-mail di contenuto attinente all'attività lavorativa:
- è fatto divieto aprire i messaggi nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus. Nel caso di messaggi provenienti da mittenti conosciuti ma che contengono allegati sospetti (file con estensione.exe .scr .pif .bat .cmd), questi ultimi non devono essere aperti. Fare attenzione a mail che contengono errori di ortografia o usano una sintassi "sconclusionata". Molto spesso i virus generano il testo del corpo mail con parte di messaggi diversi o che vengono tradotti in varie lingue in maniera approssimativa;

- è obbligatorio verificare la corretta identità dell'indirizzo del mittente quando il contenuto della mail richiede pagamenti, trasmissione di credenziali, accessi a piattaforme. Nel caso di richieste di pagamenti tramite mail, verificare la veridicità delle informazioni contattando telefonicamente il mittente/presunto mittente della stessa NON utilizzando link, indirizzi mail o numeri telefonici riportati nel messaggio;
- è opportuno utilizzare, nel caso di invio di allegati pesanti, i formati compressi (zip, rar, jpg);
- è preferibile utilizzare, nel caso in cui si debba inviare un documento all'esterno, un formato protetto da scrittura e modifiche (ad esempio il formato Acrobat pdf);
- mantenere la casella di posta in ordine cancellando documenti inutili e soprattutto allegati ingombranti. È obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti web o ftp non conosciuti);
- è concesso utilizzare per la trasmissione di file tra i dipendenti/collaboratori la posta elettronica, prestando attenzione alla dimensione degli allegati. È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi; potrebbero venir resi disponibili anche indirizzi condivisi tra più lavoratori, rendendo così chiara la natura non privata della corrispondenza;
- è fatto divieto accedere a caselle di posta elettronica personali attraverso la rete e le apparecchiature del Titolare. Il dipendente non potrà, peraltro, inoltrare automaticamente i messaggi ricevuti all'indirizzo di posta elettronica comunale su indirizzi personali;
- la posta elettronica in uscita inviata a più destinatari è inviata in maniera da rendere visibile a ciascun destinatario solo il proprio indirizzo;
- sono poi previsti, in caso di assenza del lavoratore, messaggi di risposta automatica con le coordinate di altri lavoratori cui rivolgersi. Il datore mette infine l'assegnatario dell'account in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto dei messaggi a lui indirizzati e a inoltrare al titolare quelli ritenuti rilevanti per l'ufficio in caso di assenza prolungata o non prevista e di improrogabili necessità legate all'attività lavorativa;
- la mail comunale dovrà riportare la firma corretta, con i dati del lavoratore, compresa la sua mansione, e dell'Ente così come disposto dalla direzione. La firma dovrà sempre avere il disclaimer della privacy, impostata di default al momento dell'impostazione dell'account. "Le informazioni contenute nella presente comunicazione e i relativi allegati possono essere riservate e sono, comunque, destinate esclusivamente ai destinatari sopraindicati. La diffusione, distribuzione e/o copiatura del documento trasmesso da parte di qualsiasi soggetto diverso dal destinatario è proibita, sia ai sensi dell'art. 616 c.p., che ai sensi del Regolamento Europeo 679/2016. Se avete ricevuto questa mail per errore, vi preghiamo di distruggerlo e di informarci immediatamente inviando un messaggio al mittente".
- ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per l'Ente deve essere visionata o autorizzata dal Titolare del Trattamento. La documentazione elettronica che costituisce per il Titolare "know how" comunale tecnico o

commerciale protetto, e che, quindi, viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto a tutela del patrimonio dell'Ente, non può essere comunicata all'esterno senza preventiva autorizzazione. È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti tradizionali o della posta certificata.

È inoltre espressamente vietato, salvo autorizzazione espressa del Titolare del Trattamento salvare/stampare/inoltrare documentazione comunale non necessaria allo scopo lavorativo. A titolo esemplificativo e non esaustivo è vietato:

- stampare mail aziendali per scopi personali;
- inviare informazioni sensibili ad indirizzi di posta personali;
- fotocopiare/scansionare documentazione comunale per scopi personali;
- inoltrare a terzi estranei all'Ente documentazione interna/informazioni ricevute per mezzo di strumenti informatici, salvo che non sia funzionale allo svolgimento di prestazioni professionali a favore dello stesso;
- trasmettere password, credenziali, informazioni aziendali riservate e che potrebbero comportare rischi per l'Ente e/o per i clienti/utenti dello stesso.

ACCESSO ALLA POSTA ELETTRONICA DA WEBMAIL O TRAMITE I PROPRI DISPOSITIVI PERSONALI

Le regole stabilite nel presente documento della presente procedura sono riferibili, in relazione alle sole applicazioni aziendali, anche per l'utilizzo della posta elettronica tramite piattaforma web e/o utilizzo della stessa attraverso dispositivi personali. La posta scaricata nel telefono personale o dispositivo personale, dietro espressa autorizzazione scritta del Titolare del Trattamento, va utilizzata secondo le disposizioni di cui sopra. Nell'utilizzo della posta comunale attraverso dispositivi diversi da quelli aziendali, è obbligo per l'utente verificare che tutte le comunicazioni siano sempre nella disponibilità del Titolare anche attraverso soluzioni come l'invio alla propria casella di posta.

UTILIZZO DEL PERSONAL COMPUTER (PC)

Il Personal Computer, fisso e/o portatile, affidato all'utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire a innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. L'accesso al computer è protetto da una password che deve essere custodita con la massima diligenza e non divulgata. La password va gestita secondo le modalità previste dal presente regolamento. È specificato che l'utente è responsabile per il proprio computer e per l'uso che ne viene fatto. Solo il Titolare del Trattamento, o persona specificatamente autorizzata, ha la facoltà di accedere al dispositivo al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività comunale nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio in caso di prolungata assenza od impedimento dell'incaricato e nel caso non sia stato nominato un sostituto a questa funzione, informando tempestivamente l'incaricato dell'intervento di accesso realizzato.

Si ribadisce che:

- non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione esplicita del Titolare del Trattamento e di programmi non originali. L'inosservanza della presente disposizione espone lo stesso Ente a gravi responsabilità civili; si evidenzia, inoltre, che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o

comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate penalmente e possono anche comportare il sorgere di una responsabilità amministrativa a carico dell'Ente, come disposto dall'art. 25-nonies del D.lgs. 8 giugno 2001, n. 231, con applicazione di sanzioni pecuniarie.

- non è consentito modificare le caratteristiche impostate sul proprio PC, salvo previa autorizzazione esplicita del Titolare del Trattamento;
- non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, …), se non con l'autorizzazione espressa del Titolare del Trattamento;
- il PC deve essere sempre mantenuto in posizione idonea e sicura affinché si evitino cadute e rotture dovute a urti accidentali;
- il PC va mantenuto pulito e nella massima efficienza. È cura dell'incaricato a cui lo stesso è affidato provvedere alla pulizia dei file e del materiale non più necessario in modo da mantenere il PC perfettamente operativo;
- in caso di malfunzionamento, manutenzione straordinaria, incidente, o problemi che si possano riscontrare nel PC, l'incaricato dovrà confrontarsi con il Titolare del Trattamento e non intervenire in modo autonomo.

UTILIZZO DEI PC PORTATILI

L'incaricato del trattamento è responsabile del computer portatile (notebook) e/o di ulteriori dispositivi eventualmente assegnatogli temporaneamente o stabilmente dal Titolare e deve custodirlo con diligenza, sia durante gli spostamenti fuori dell'azienda, sia durante l'utilizzo nel luogo di lavoro. Premesso che l'utilizzo di tali dispositivi è limitato all'utente assegnatario è vietato cederne l'uso, anche temporaneo, a terzi.

Ai computer portatili si applicano tutte le regole di utilizzo previste per i PC connessi in rete. L'incaricato al quale è stato assegnato temporaneamente un PC portatile, deve prestare particolare attenzione a provvedere alla rimozione di eventuali file personali sul portatile prima della sua riconsegna all'Ente che al rientro provvederà per mano del Titolare ad un controllo sulla sua efficienza e funzionalità. I PC portatili utilizzati all'esterno della sede dell'Ente (in occasione di trasferte, fiere, convegni, riunioni, ecc.), in caso di allontanamento dell'utente dalla macchina devono essere custoditi in un luogo protetto. Eventuali configurazioni di accesso remoto, dirette verso la rete del Titolare o attraverso Internet, devono essere autorizzate esclusivamente dal Titolare del Trattamento o da suo delegato.
È fatto salvo l'obbligo di comunicare all'Ente eventuali guasti o anomalie, riscontrate nell'uso dei dispositivi, e informare tempestivamente di eventuali smarrimenti o furti. L'eventuale perdita o sottrazione del dispositivo costituisce una forma di "data breach", ovvero di violazione dei dati personali o, potrebbe costituire, comunque, un serio rischio per la conoscibilità a terzi non autorizzati dei dati personali in esso contenuti.

UTILIZZO DEL TELEFONO CELLULARE

Il telefono cellulare comunale affidato all'utente è uno strumento di lavoro. Quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. L'uso del telefono è consentito esclusivamente per lo svolgimento dell'attività lavorativa e ne rimane vietato l'utilizzo per l'invio e la ricezione di messaggi di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa.

Non sono soggetti a tale disciplina i telefoni cellulari concessi dall'Ente in uso promiscuo a titolo di benefit. È obbligo in questo caso adottare ogni cautela al fine di garantire un trattamento conforme dei dati aziendali, adottando ogni misura necessaria al fine, compreso il divieto di condivisione del telefono con soggetti terzi, e attenersi alle disposizioni del paragrafo di cui sopra per la riconsegna dello stesso. Il Titolare sottolinea che al fine di valutare il contratto con il fornitore di servizi telefonici, potranno essere trattare alcune informazioni relative alle chiamate in uscita effettuate dai dipendenti, così come disposto dal Garante della Privacy e solo per finalità esplicite e definite che non ricomprendono la possibilità di controllo a distanza sui lavoratori. L'utilizzo del proprio cellulare personale durante l'orario di lavoro è consentito laddove ricorrano ragioni di necessità e/o urgenza. L'utilizzo deve essere comunque improntato a criteri di buona fede e correttezza e non può in alcun caso pregiudicare il disbrigo assiduo e diligente delle mansioni assegnate.

UTILIZZO DEI DISPOSITIVI PERSONALI PER FINI LAVORATIVI (BYOD BRING YOUR ON DEVICE)

È opportuno precisare che, qualora sul dispositivo di uso "ibrido" siano presenti dati o informazioni aziendali qualificabili come personali e riservati, per i quali l'Ente riveste il ruolo di Titolare del trattamento, vige l'obbligo di porre in essere gli adempimenti previsti dal Regolamento Europeo e dalla normativa di riferimento vigente. L'utilizzo per finalità lavorative attraverso i propri dispositivi personali dovrà essere concordato con il Titolare del Trattamento. Nei casi autorizzati, verrà di volta in volta predisposto un disciplinare di utilizzo con le misure di sicurezza idonee a garantire la massima protezione delle informazioni. È fatto divieto, altresì, utilizzare i propri dispositivi per accedere al materiale comunale attraverso password e credenziali anche personali, scaricare la posta elettronica, accedere in remoto a server e cloud aziendali.

UTILIZZO E SMALTIMENTO DEI SUPPORTI DI MEMORIZZAZIONE ADOPERATI

I supporti di memorizzazione come CD, DVD, hard disk esterni, memory card, pen drive hanno precise regole di impiego. Il loro utilizzo deve essere effettuato con molta cautela e solo per motivi attinenti le attività aziendali. È opportuno valutare periodicamente, con specifici sistemi, la presenza o meno di virus all'interno del supporto e comunque prima di ogni utilizzo.

È da evitare il salvataggio su tali supporti di dati particolari, giudiziari, strategici e riservati per il Titolare.

Se i supporti devono essere reimpiegati o riciclati, si dovranno adottare alcune misure di sicurezza quali tecniche preventive per la memorizzazione sicura dei dati (Cifratura manuale o automatica di singoli file o gruppi di file); tecniche per la cancellazione sicura dei dati ottenibile con programmi informatici, formattazione "a basso livello" dei dispositivi di tipo hard disk (low-level formatting–LLF), demagnetizzazione (degaussing) dei dispositivi di memoria basati su supporti magnetici o magneto-ottici). Se i supporti devono essere smaltiti invece si dovranno adottare per esempio sistemi di punzonatura o deformazione meccanica, distruzione fisica o disintegrazione (usata per i supporti ottici come i cd-rom e i dvd), o demagnetizzazione ad alta intensità.

CONNESSIONE DA REMOTO (VPN E ALTRE TIPOLOGIE)

TELEASSISTENZA

Relativamente alle attività di manutenzione remota su personal computer connessi alla rete comunale, il personale tecnico della società informatica formalmente incaricata potrà utilizzare specifici software. Tali programmi vengono utilizzati per assistere l'utente durante la normale attività informatica ovvero per svolgere manutenzione su applicativi e su hardware.

L'attività di assistenza e manutenzione avviene previa autorizzazione telefonica da parte dell'utente interessato. La configurazione del software prevede un indicatore visivo sul monitor dell'utente che indica quando il tecnico è connesso al personal computer.
Le disposizioni del presente Regolamento si applicano, per quanto compatibili, anche alle ipotesi di collegamento alla rete comunale da postazioni esterne all'ufficio (ad esempio: collegamento da casa o collegamento presso i locali della Società cliente/fornitore).

SMART WORKING/TELELAVORO

Il Titolare per garantire continuità lavorativa al fine di adempiere agli obblighi contrattuali con i propri clienti e altresì garantire adeguate misure di sicurezza per i propri dipendenti/collaboratori potrebbe predisporre collegamenti da remoto effettuati tramite VPN (Virtual Private Network) sicura al fine dell'attivazione dello smart working, ovvero per consentire la gestione del lavoro da casa. Tale modalità di lavoro sarà attivata sulla base di specifiche individuate dal Titolare.

GESTIONE DELL'ACCOUNT DI POSTA ELETTRONICA SUCCESSIVAMENTE ALLA CESSAZIONE DEL RAPPORTO DI LAVORO E/O COLLABORAZIONE

ACCOUNT PERSONALE

Successivamente alla cessazione del rapporto di lavoro e/o collaborazione la casella di posta elettronica sarà disattivata. A partire da tale data non sono consentiti né l'accesso alla casella, né la ricezione tramite inoltro. Casi particolari devono essere esplicitamente autorizzati dalla direzione comunale. Sarà inoltre predisposto temporaneamente un sistema di risposta automatica per informare il mittente dell'avvenuta disattivazione dell'account di posta elettronica e dare indicazione del nuovo referente se necessario. Il contenuto degli account di posta elettronica disattivata sarà registrato in un file di backup. Successivamente alla cessazione del rapporto di lavoro e/o collaborazione, il Titolare potrà liberamente accedere al contenuto del file di backup, del personal computer nonché alla casella di posta elettronica assegnata al lavoratore durante il rapporto di lavoro nel caso di ragionevoli motivi come quelli di continuità dell'attività del Titolare, per finalità di sicurezza del sistema informatico, nonché quando ciò dovesse risultare necessario anche per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

ACCOUNT CONDIVISO

Nel caso di account condiviso, utilizzato da più persone all'interno di uno stesso reparto/settore, lo stesso continuerà ad essere utilizzato sia da eventuali sostituto alla mansione che dai colleghi. Sarà cura dell'interessato, ovvero del Titolare, avvisare che la risorsa non sarà più disponibile a quell'account con le ulteriori disposizioni prese a tal riguardo. Le informazioni e la documentazione riferibile a quell'account continuerà a essere nella disponibilità del Titolare e dei colleghi per garantire la continuità lavorativa.

ACCESSO ALLA POSTA ELETTRONICA NELL'AMBITO DEL PROGRAMMA BYOD

Le regole di cui sopra sono applicabili, in relazione alle sole applicazioni aziendali, anche per l'utilizzo della posta elettronica nell'ambito del programma BYOD.

PISHING

Il phishing è una tecnica illecita utilizzata per appropriarsi di informazioni riservate relative a una persona o a un'azienda - username e password, codici di accesso (come il PIN del cellulare), numeri di conto corrente, dati del bancomat e della carta di credito – con l'intento di compiere operazioni fraudolente.

La truffa avviene di solito via e-mail, ma possono essere utilizzati anche sms, chat e social media. Il «ladro» si presenta, in genere, come un soggetto autorevole (banca, gestore di carte di credito, ente pubblico, ecc.) che invita a fornire dati personali per risolvere particolari problemi tecnici con il conto bancario o con la carta di credito, per accettare cambiamenti contrattuali o offerte promozionali, per gestire la pratica per un rimborso fiscale o una cartella esattoriale, ecc. In genere, i messaggi di phishing invitano a fornire direttamente i propri dati personali, oppure a cliccare un link che rimanda ad una pagina web dove è presente un form da compilare. I dati così carpiti possono poi essere utilizzati per fare acquisti a spese della vittima, prelevare denaro dal suo conto o addirittura per compiere attività illecite utilizzando il suo nome e le sue credenziali.

Al fine di prevenire rischi derivanti da spam e pishing, è consigliabile non diffondere la mail comunale in internet, come anche il numero di cellulare comunale, fare sempre attenzione a link e allegati, diffidare delle richieste di qualsiasi codice di accesso che permetta di entrare in un servizio o account: nome utente, password, PIN, codice di sicurezza, come del resto di dati bancari o di codici di carta di credito. I messaggi di phishing sono progettati per ingannare e spesso utilizzano imitazioni realistiche dei loghi o addirittura delle pagine web ufficiali di banche, aziende ed enti. In questo caso valutare la presenza o meno di errori grammaticali, anche grossolani, di formattazione o di traduzione da altre lingue, e prestare attenzione ai toni. I messaggi con toni intimidatori, che ad esempio contengono minacce di chiusura del conto bancario o di sanzioni se non si risponde immediatamente, possono essere subdole strategie per spingere il destinatario a fornire informazioni personali.

Oltre a tenere aggiornato sul pc o sullo smartphone un programma antivirus che protegga anche dal phishing, è consigliato di non memorizzare dati personali e codici di accesso nei browser utilizzati per navigare online. In ogni caso, è buona prassi impostare password alfanumeriche complesse, cambiandole spesso e scegliendo credenziali diverse per ogni servizio utilizzato: banca online, e-mail, social network.

Le stesse attenzioni sono da tenere anche nell'utilizzo della PEC (Posta Elettronica Certificata), considerata di default sicura ma che, in realtà, non lo è.

Qualora si ravvisassero casi di spam o di phishing è necessario segnalare l'accaduto al Titolare in tempi utili al fine di poter evitare rischi per lo stesso e i dati contenuti nei dispositivi del Titolare.

DOCUMENTI PERSONALI ALLA CONCLUSIONE DEL RAPPORTO

Alla chiusura del rapporto di lavoro, all'interessato vanno consegnati tutti i documenti contenenti i propri dati, ad esclusione di quelli che l'Ente deve trattenere per obblighi di legge e per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Nel caso non fosse possibile trattare direttamente con l'interessato, si deve mandare un avviso per il ritiro. Nel frattempo i materiali da consegnare vanno posti in busta chiusa e al ritiro degli stessi va fatta firmare una ricevuta di consegna.

Se passato un lasso di tempo ragionevole, l'interessato o un suo delegato non si presenterà a ritirarli, si avvierà una procedura di distruzione dei documenti, se possibile certificata ovvero documentata, ovviamente valutando prima se ci sono documenti che non sia opportuno eliminare (ad. es documenti in originale unici, ecc). In ogni caso ogni documento

e/o fascicolo che transiti dall'archivio corrente a quello storico, deve essere prima depurato di tutti i dati personali non più necessari.

NORME FINALI

Le disposizioni del presente regolamento si applicano, per quanto compatibili, anche alle ipotesi di collegamento alla rete comunale da postazioni esterne all'ufficio (ad esempio: collegamento da casa).

ACCESSO AI DATI TRATTATI DALL'UTENTE

L'Ente promuove ogni opportuna misura organizzativa, tecnologica e di sicurezza volta a prevenire il rischio di utilizzi indebiti che possano generare responsabilità di natura civile o penale oltre a "minimizzare" l'uso di dati riferibili ai lavoratori e collaboratori e a garantire la disponibilità e l'integrità dei sistemi informatici e dei dati. Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi aziendali comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà del Titolare, tramite addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

CONTROLLI ORDINARI E STRAORDINARI

Il mancato rispetto delle indicazioni in materia di uso delle risorse aziendali conferite ai dipendenti espone gli stessi a provvedimenti disciplinari e risarcitori previsti dal vigente CCNL, nonché a tutte le azioni civili e penali consentite
Mentre il controllo ordinario è prettamente di natura anonima e serve per individuare la causa di eventuali problematiche che dovessero insorgere all'interno della rete informatica, il controllo straordinario risulta necessario nel caso in cui il comportamento anomalo e ripetuto nel tempo, nei casi di maggiore gravità (es. accesso a siti illegali o a contenuto discriminatorio o violento) e nei casi di indagini di natura difensiva ovvero nel caso in cui sia necessario accertare, comportamenti che possano costituire reato o che siano comunque illeciti o non conformi alle disposizioni aziendali.
Il controllo straordinario può avvenire anche mediante accesso diretto al PC del dipendente che, su richiesta, dovrà consegnarlo al Titolare del Trattamento. Il controllo straordinario, che potrà avvenire anche con la collaborazione di professionisti esterni, non potrà avere ad oggetto un arco temporale eccedente i sei mesi precedenti la data in cui esso viene effettuato, salva la necessità di estendere l'indagine oltre tale periodo in ragione della natura del comportamento oggetto di indagine e/o in conseguenza di fatti emersi nel controllo relativo ai sei mesi precedenti la data dell'indagine.

CESSAZIONE DELLA DISPONIBILITÀ DEI SERVIZI INFORMATICI AZIENDALI

Ai sensi del presente regolamento, la disponibilità dei servizi informatici aziendali cesserà totalmente nel caso non sussista più la condizione di dipendente o di collaboratore. Altresì può essere cessata o limitata nei privilegi assegnati in caso di:

- revoca dell'autorizzazione all'uso a seguito di un cambio di mansione;
- accertato uso non corretto o comunque estraneo alla sua attività lavorativa dei servizi informatici aziendali;
- accertate manomissioni e/o interventi illeciti sul hardware e/o sul software;

- accertate diffusione o comunicazione imputabili direttamente o indirettamente all'utente, di password, procedure di connessione, indirizzo I.P. e altre informazioni tecniche riservate;
- accesso illecito e intenzionale dell'utente a directory, a siti e/o file e/o servizi da chiunque resi disponibili, in particolare se l'attività dell'utente comporti danno, anche solo potenziale al sito contattato;
- violazione delle regole essenziali stabilite dal presente regolamento.

Si ricorda inoltre che, una volta cessata la condizione di dipendente o collaboratore è vietato asportare dati aziendali prodotti nell'attività istituzionale. Non sarà dato seguito, pertanto, alla richiesta di scarico massivo (per es. su supporto esterno) delle mail dell'utente, né di altri file contenuti nei file server o nei personal computer

RESPONSABILITÀ DELL'INCARICATO E/O DELL'UTILIZZATORE DELLE RISORSE INFORMATICHE

Il dipendente/collaboratore è direttamente e totalmente responsabile delle modalità in cui opera e dell'uso che egli fa del servizio di posta elettronica e di accesso a Internet, dei contenuti che vi ricerca, dei siti che contatta, delle informazioni che tratta.

Premesso che il trattamento delle informazioni e l'utilizzo delle stesse con modalità informatiche e non è consentito solo per lo svolgimento delle mansioni lavorative, con l'accettazione di questo regolamento l'utente è informato e consapevole del fatto che la conoscenza della password da parte di terzi consente a questi ultimi l'accesso alla rete comunale e l'utilizzo dei relativi servizi in nome dell'utente e l'accesso ai dati cui il medesimo è abilitato, con le conseguenze che la cosa può comportare, quali ad esempio la visualizzazione di informazioni riservate, la distruzione o la modifica dei dati, la lettura della propria posta elettronica, l'uso indebito di servizi ecc. Lo stesso prende atto che è vietato servirsi o dar modo ad altri di servirsi della rete comunale e dei servizi da essa messi a disposizione per utilizzi illeciti che violino o trasgrediscano diritti d'autore, marchi, brevetti, comunicazioni private o altri diritti tutelati dalla normativa corrente, per utilizzi contro la morale e l'ordine pubblico, per recare molestia alla quiete pubblica o privata, per recare offesa o danno diretto o indiretto all'Ente o a terzi.

SOCIAL MEDIA

FINALITA'

Questo paragrafo mira a regolare la relazione su internet, e in particolare sui social media, tra l'Ente e i suoi dipendenti.

La Social Media Policy fornisce le principali norme di comportamento che tutto il personale ed eventualmente i professionisti esterni, sono tenuti ad osservare quando utilizzano i social media e pubblicano contenuti e commenti, sia che questo faccia parte del proprio lavoro e avvenga tramite un account comunale sia quando attraverso un account personale si parla direttamente o indirettamente dell'attività o del ruolo svolto all'interno dell'Ente.

Considerando che l'utilizzo scorretto dei canali social può danneggiare, anche gravemente, l'immagine e la reputazione del Titolare e, di conseguenza, delle figure professionali che vi lavorano e premesso che ognuno può liberamente condividere sui propri profili privati i contenuti diffusi dal Titolare, rimane vietata la diffusione sul proprio profilo privato di contenuti o eventi dell'Ente non precedentemente segnalati o comunque non presenti sul sito ufficiale. È bene ricordare che sui social media voi rappresentate e/o potrete essere identificati con il Titolare o le attività dello stesso se partecipate a un forum di discussione, a un gruppo o un network che si riferisce al Titolare, se parlate e commentate della stessa, se caricate foto o video mentre state svolgendo la vostra attività lavorativa, se parlate con le persone con cui lavorate di eventi di lavoro o qualsiasi evento a cui è associato l'Ente.

Per queste ragioni è necessario avere una policy che offra linee guida per quanto riguarda le aspettative del Titolare e che definisca le responsabilità dei dipendenti e licenziatari quando utilizzano i social media per motivi di lavoro o a titolo personale.

Tali linee si indirizzano in 2 aree:

- L'uso personale dei Social Media
- L'uso professionale dei Social Media

Premesso che tutto ciò che viene pubblicato su internet può essere letto da tutti, ognuno è invitato a pensare a quello che scrive nello stesso modo in cui lo farebbe per comunicare con le persone che non conosce personalmente.

In particolare, occorre tenere conto delle seguenti linee guida:

- Non devono essere scaricate e/o pubblicate immagini offensive o inappropriate;
- Non devono essere scaricati e/o pubblicati commenti offensivi o inappropriati;
- Non devono essere pubblicati commenti offensivi o inappropriati su colleghi o clienti;
- Non si deve fare alcun riferimento a qualsiasi affiliazione a organizzazioni politiche;
- Le informazioni riservate non devono mai essere divulgate;
- I dipendenti non devono mai accedere né utilizzare qualsiasi sito web o servizio riprovevole o illegale utilizzando i dispositivi messi a disposizione dal Titolare;
- Altresì si ribadisce che non è consentito divulgare attraverso i social media informazioni riservate, come la corrispondenza interna, informazioni di terze parti di cui è a conoscenza (ad esempio partner, istituzioni, clienti/utenti, stakeholder, ecc.) o informazioni su attività lavorative, servizi, progetti e documenti non ancora resi pubblici, decisioni da assumere e provvedimenti relativi a procedimenti in corso, prima che siano stati ufficialmente deliberati e comunicati formalmente alle parti interessate;
- Fermo restando il corretto esercizio del diritto di critica, non è consentito pubblicare e trasmettere messaggi minatori o ingiuriosi, commenti e dichiarazioni pubbliche offensive nei confronti del Titolare, o riferiti alle attività dello stesso e più in generale al suo operato, che per forme e contenuti possono nuocere ledendo l'immagine o compromettendone a vario titolo l'efficienza e l'operatività. È opportuno ricordare che i contenuti anche se privati, una volta messi in rete possono avere risonanza globale;
- È obbligo rispettare la privacy dei colleghi, evitando riferimenti all'attività lavorativa svolta, fatte salve le informazioni di dominio pubblico e non è consentito divulgare foto, video, o altro materiale multimediale, che riprenda locali e personale senza l'esplicita autorizzazione delle strutture e delle persone coinvolte;
- È vietato aprire blog, pagine o altri canali a nome del Titolare o che trattino argomenti riferiti all'attività della stessa, senza autorizzazione preventiva della direzione e utilizzare su account personali il marchio dell'Ente.

Le indicazioni si applicano quando un dipendente utilizza i Social Media per lavoro o per uso personale e viene specificamente indicato l'Ente o quando il dipendente si identifichi come un dipendente dello stesso. È inoltre applicabile anche quando è ragionevole desumere, dalle informazioni pubblicate, che il dipendente si riferisce all'Ente, ai suoi colleghi e/o ai clienti/utenti dello stesso.

Qualora l'uso di canali di Social Media sia insito nel ruolo lavorativo del dipendente, l'uso personale dei Social Media deve avvenire esclusivamente nel tempo libero e non deve includere l'uso dell'indirizzo e-mail comunale (qualora il dipendente ne abbia uno).

USO PROFESSIONALE

Quando i dipendenti utilizzano i Social Media per attività di lavoro consentite gli stessi devono:

- essere molto cauti con i Social Media o i media legati ai consumatori quando cercano di promuovere nell'opinione pubblica l'immagine del Titolare;
- rispettare sempre la riservatezza e le preferenze di contatto di ogni individuo ed essere consapevoli del fatto che alcune persone non vogliono essere contattate tramite i canali dei Social Media.

RESPONSABILITÀ

I dipendenti devono tenere presente che i clienti/utenti, gli altri dipendenti, i fornitori e le Autorità Pubbliche possono avere accesso ai contenuti on-line che sono pubblicati. I dipendenti sono personalmente responsabili per i contenuti che pubblicano on-line. I dipendenti devono assicurarsi che:

- tutte le informazioni fornite sui prodotti e i servizi siano realmente precise;
- se un dipendente esprime un commento o un'opinione su un particolare argomento e lo stesso si identifica come un dipendente del Titolare, deve essere chiaro che i contenuti non sono espressi per conto dello stesso ma rappresentano solo le proprie convinzioni.

In ogni momento, il Titolare si riserva il diritto di monitorare i Social Media e intervenire laddove i commenti di un dipendente potrebbero potenzialmente influire sui rapporti con i partner, i fornitori e/o i clienti o tra colleghi.

MESSAGGISTICA ISTANTANEA

Partendo dall'assunto che gli strumenti di messaggistica istantanea non danno alcuna garanzia legale sull'identità della persona a cui si trasmettono informazioni, si desume che è sempre un rischio utilizzarli in contesti particolari come quello del trattamento di dati soprattutto se relativi a informazioni aziendali, accordi contrattuali e precontrattuali, ecc. Premesso quindi che nelle chat o nei messaggi non c'è modo per avere una minima sicurezza su chi c'è dall'altra parte, è fatto divieto utilizzare sistemi di messaggistica istantanea, come Skype, Facebook, Whatsapp e Telegram, e ogni nuova applicazione che potrebbe essere assimilata al funzionamento a queste, per l'invio di informazioni aziendali, soprattutto se rientranti tra quelle riservate o che l'Ente ritiene di voler tutelare.

È altresì fatto divieto di utilizzare sul dispositivo comunale un qualsiasi tipo di applicazione di messaggistica istantanea personale. Nel caso dovesse emergere la necessità di utilizzo delle stesse, il Titolare del Trattamento provvederà allo sviluppo di un account comunale adibito per l'utilizzo a fini lavorativi, pur con il divieto di trasmissione di informazioni riservate aziendali. Altresì nell'utilizzo di messaggistica istantanea è obbligatorio prestare sempre attenzione alla possibilità di incorrere in virus informatici che potrebbero circolare nei contatti presenti in rubrica. Si ricorda che è pericoloso aprire un link arrivato da un mittente sconosciuto e file ricevuti da persone sospette in quanto potrebbero essere malware che mettono a rischio le informazioni contenute nel dispositivo, ma anche la rete informatica a cui il dispositivo è collegato.

APPLICAZIONI

Il modo migliore per veicolare un malware nello smartphone è attraverso una app malevola ed è quindi opportuno fare attenzione a cosa scarichiamo e da dove. Nel caso in cui nel dispositivo personale siano conservate informazioni aziendali, immagini, mail, contatti di clienti/utenti e fornitori del Titolare, nell'utilizzo di applicazioni che richiedono l'accesso ai dati è obbligo prestare sempre molta attenzione a capirne le finalità e i soggetti terzi con cui verranno condivisi.

RACCOLTA E GESTIONE DEI LOG

Un log è la registrazione di ogni attività eseguita su un dispositivo elettronico. Esso normalmente riporta indicazioni temporali, riferimenti all'attività effettuata e riferimenti a chi l'ha eseguita; gli eventi vengono quindi registrati e memorizzati, dando origine a quelli che vengono definiti come file di log. Pertanto, i file di log sono uno strumento capace di rappresentare con precisione le operazioni compiute sui sistemi informatici e quindi sui dati personali. Essi consentono di garantire la sicurezza dell'infrastruttura informatica.

I file di log sono uno strumento capace di rappresentare con precisione le operazioni compiute sui sistemi informatici e quindi sui dati personali. In altri termini attraverso i file di log è possibile ricostruire l'iter di operazioni che hanno riguardato un determinato sistema informativo consentendo, in particolar modo, il tracciamento delle eventuali anomalie o minacce che potrebbero colpire i sistemi compromettendo di conseguenza la sicurezza delle informazioni memorizzate negli asset informatici.

I log vengono raccolti e conservati da parte della Struttura esclusivamente per il perseguimento delle seguenti finalità:

- Conformità alle normative vigenti e applicabili;
- Monitoraggio dei sistemi informatici al fine di rilevare eventuali violazioni nel loro utilizzo e permettere quindi la possibilità di svolgere analisi post-incidente;
- Monitoraggio dei sistemi informatici della Struttura (troubleshooting), al fine di garantire la continuità dei servizi erogati mediante la rilevazione di anomalie di funzionamento e la loro risoluzione;
- Adempimenti contrattuali, quando previsto.

Rilevanza Legale dei File Log

A seguito del diffusissimo utilizzo di software, siti web e app, i *file di log* hanno ormai acquisito un'importante rilevanza legale. Infatti, come già detto**,** i log spesso forniscono elementi di evidenza probatoria (in informatica forense) dovendo testimoniare eventuali comportamenti illeciti, oppure, in altri casi, possono fornire prove di esplicita acquisizione del consenso dell'interessato. In relazione a quest'ultimo punto si inserisce il tema del c.d. *Point&Click,* ovvero la conferma di una espressa richiesta di accettazione tramite la spunta di un'apposita casella ("point") con un click del pulsante del *mouse* ("click"). A tale proposito recenti orientamenti giurisprudenziali in ambito civilistico, basandosi sul principio della libertà delle forme nella conclusione dei contratti, seppur con evidenti e rilevanti controversie, in particolar modo per l'approvazione delle clausole vessatorie e fatti salvi i casi di cui all'art. 1350 c.c., per i quali è espressamente richiesta la forma scritta, considerano la pratica del *Point&Click* un valido mezzo per la conclusione di contratti on-line. Inoltre, è acclarato, come anche confermato dal

Considerando n. 17 della Direttiva 2002/58/CE *("Il consenso può essere fornito secondo qualsiasi modalità appropriata che consenta all'utente di esprimere liberamente e in conoscenza di causa i suoi desideri specifici, compresa la selezione di un'apposita casella nel caso di un sito Internet"*), che anche il consenso in ambito privacy è valido se espresso tramite *Point&Click*.
Atteso quindi, che i contratti ed i consensi *Point&Click,* **laddove tale sistema venga utilizzato***,* possono ritenersi validi, la presenza di *file di log* può sicuramente rappresentare la prova che se sia stato effettuato un *Point&Click* da parte dell'utente e pertanto i *file di log* diventano uno strumento utile ai fini probatori.

Inoltre, a maggior conferma di quanto espresso, i *log* possono essere considerati al pari di una riproduzione meccanica (articolo 2712 del Codice Civile) e pertanto costituiscono piena prova dei fatti e delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime**.**
In concreto, in applicazione dell'art. 20, comma 1-bis del Decreto Legislativo n. 82 del 7 marzo 2005, noto come "Codice dell'amministrazione digitale", il giudice civile ha facoltà di valutare il valore probatorio del documento informatico, tenendo conto delle caratteristiche di sicurezza, integrità e immodificabilità del documento medesimo.
Sotto il profilo puramente pratico, i log file costituiscono strumenti di troubleshooting (letteralmente "eliminazione del problema"), utili ai sistemisti o agli amministratori di rete per eseguire una corretta manutenzione ed eventuale riparazione del sistema informatico.

COMUNICAZIONE ALL'INTERNO DELL'ENTE

Le comunicazioni all'interno dell'Ente saranno veicolate in modo da rendere le stesse funzionali e sicure.
All'interno della procedura che il Titolare potrebbe attivare il dipendente avrà la possibilità di selezionare una voce di preferenza tra messaggio, messaggistica istantanea WhatsApp e mail, per le comunicazioni che il titolare dovrà comunicargli. La presente modalità sarà utilizzata solo per comunicazione relative all'organizzazione e alla gestione delle attività e per programmare i servizi del Titolare. Le comunicazioni, in relazione alla delicatezza delle informazioni contenute, sono riservate e il dipendente collaboratore dovrà impegnarsi a mantenerle tutelate, anche assicurando adeguati sistemi di sicurezza alla modalità selezionata.

****

Alleg. 1

AUTORIZZAZIONE AL TRATTAMENTO DEI DATI PERSONALI E NOMINA REFERENTE PRIVACY

Egregio/a Sig./Sig.ra _____

Premesso che lei è dipendente del **Comune di Dovera** avente sede in Piazza XXV Aprile, 1 - 26010 Dovera (CR) con la mansione di _____.

Premesso che le attività a lei assegnate comportano il trattamento di dati personali e di dati particolari come definiti all'Art. 4 e all'Art. 9 del Regolamento Europeo 679/2016;

Premesso che l'attività di trattamento dei dati è disciplinata dal Regolamento UE 679/2016 e dalla disciplina vigente;

Premesso che per effetto del Regolamento Europeo UE 679/2016 il Titolare del Trattamento ha l'obbligo di adottare specifiche misure organizzative e di impartire istruzioni a tutti coloro che sono stati autorizzati al trattamento dei dati personali (Artt. 5, 24, 29 e 32).

Tutto ciò premesso

Il Titolare, al fine di organizzare la propria attività nonché garantire un'adeguata e puntuale applicazione della normativa prevista dal Regolamento UE 2016/679, la nomina REFERENTE PRIVACY in relazione all'area/funzione _____

e la autorizza al trattamento dei dati personali che tratterà nello svolgimento delle sue funzioni.

Il Comune, nella persona del Sindaco pro tempore, la autorizza al trattamento dei dati personali. Il trattamento dei dati è consentito al solo ed esclusivo fine di svolgere le mansioni a lei assegnate. Ogni altro tipo di trattamento di dati personali non è consentito. A tal fine lei è autorizzato ad utilizzare la strumentazione informatica e non messa a sua disposizione nelle modalità e in ottemperanza alla presente scrittura, al Regolamento Privacy, alle istruzioni ricevute e alle disposizioni vigenti.

NOMINA COME REFERENTE PRIVACY

Altresì, l'Ente nella persona del Sindaco pro tempore, ha provveduto a nominarla Referente Privacy. A tal fine i suoi compiti saranno

- segnalare al Titolare del Trattamento eventuali richieste ricevute da parte dell'interessato sull'esercizio dei relativi diritti, nonché attenersi alla procedura interna sull'esercizio dei diritti;

- cooperare in caso di attività di controllo in ambito privacy da parte di strutture interne o esterne, fornendo eventuale documentazione richiesta e garantendo l'accesso ai locali;
- informare il Titolare del Trattamento dell'esistenza di un nuovo progetto che impatta sulla protezione dei dati, in applicazione del principio di privacy by design e by default;
- informare il Titolare del Trattamento dell'esistenza di un nuovo trattamento per cui risulta necessario aggiornare il registro o modificarlo, in applicazione del principio di privacy by design e by default;
- informare il Titolare del Trattamento della presenza di una nuova risorsa che tratta dati personali al fine di valutare necessità di formazione in ambito privacy;
- controllare che le persone autorizzate al trattamento rispettino le indicazioni impartite dall'Ente;
- segnalare casi di mancato rispetto delle disposizioni in tema di protezione dei dati al Titolare del Trattamento;
- sorvegliare l'osservanza della normativa in materia di privacy e vigilare sull'effettivo funzionamento delle prescrizioni adottate dall'Ente;
- sorvegliare l'osservanza della normativa in materia di privacy dei Responsabili Esterni del Trattamento e vigilare sull'effettivo funzionamento delle prescrizioni che devono essere adottate dall'Ente;
- aggiornare l'elenco delle Società che svolgono funzione Responsabili Esterni del Trattamento, a qualsiasi titolo. L'elenco dovrà essere sempre disponibile e messo a disposizione nel caso di richiesta di clienti, interessati e per le autorità di controllo;
- informare e fornire consulenza al Titolare del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dalla normativa in materia privacy;
- ricevere e dare esecuzione alle istruzioni e alle prescrizioni impartite dal Consulente Privacy eventualmente incaricato e/o dal DPO;
- predisporre e attuare adeguati flussi di comunicazione da e verso il Consulente Privacy e/o il DPO, ivi inclusi gli alert/data breach di sistema;
- fungere da punto di contatto per gli interessati relativamente a tutte le questioni inerenti il trattamento dei loro dati personali e all'esercizio dei diritti;
- cooperare con il Titolare nella redazione e nell'aggiornamento del Registro delle Attività di Trattamento.

Il titolare del trattamento comunica con la presente che la mancata osservanza di tali istruzioni può far sorgere in capo all'incaricato responsabilità penale per la mancata adozione delle misure minime di sicurezza, responsabilità civile nei confronti di terzi che venissero danneggiati dalla perdita, distruzione e utilizzazione illecita dei dati e responsabilità contrattuale nei confronti del datore di lavoro.

Nell'espletamento delle sue mansioni lavorative lei ha l'obbligo di trattare i dati anche particolari, tra cui quelli relativi alla salute, e tutti i dati personali di cui viene a conoscenza in modo lecito e secondo correttezza, mantenendo assoluto riserbo. È fatto assoluto divieto comunicare, diffondere, utilizzare i dati personali provenienti dalle banche dati e dagli archivi in assenza di autorizzazione del titolare e comunque nei casi non consentiti dalla legge.

Nello specifico lei è autorizzato ad accedere ai dati, conservati sia in formato elettronico che cartaceo, alle seguenti cartelle presenti sul server

ad utilizzare i seguenti software/applicativi

limitatamente alle informazioni previste dal suo profilo e autorizzate dal Titolare del Trattamento.

Lei può accedere alle cartelle e utilizzare i suddetti gestionali/applicativi con le credenziali che le sono state fornite. Le stesse sono strettamente personali e non possono essere comunicate a terzi. Qualsiasi operazione effettuata attraverso l'inserimento di credenziali identificate dal sistema informatico di riconoscimento viene ricondotta al titolare delle medesime credenziali, indipendentemente dalla postazione di lavoro utilizzata, salvo che lo stesso titolare delle credenziali non fornisca prova contraria. L'elenco degli accessi viene conservato dal sistema informatico per un periodo non inferiore ai 6 (sei) mesi e non superiore ai 12 (dodici) mesi e può essere consultato dal Titolare del Trattamento in caso di necessità e motivi di sicurezza ovvero per motivi di pubblico interesse o connessi all'esercizio di pubblici poteri.

Le è fatto altresì divieto comunicare agli altri incaricati ed a terzi, anche in modo indiretto, le proprie credenziali di autenticazione e le proprie password di accesso ai dispositivi aziendali.

UTILIZZO DELL'ACCOUNT ISTITUZIONALE

Ai fini delle mansioni a lei attribuite, è autorizzato a utilizzare i seguenti account

Ad uso esclusivo
Ad uso condiviso

Premettendo che i soggetti esterni possono attribuire carattere istituzionale alla corrispondenza ricevuta attraverso suddetti account, si ribadisce che per l'utilizzo degli stessi dovrà tenere in debito conto le istruzioni impartite dal Titolare nonché le cautele espresse nella Policy dell'Ente.

ISTRUZIONI PER GLI INCARICATI

La Persona Autorizzata dovrà effettuare il Trattamento dei dati nel rispetto della normativa vigente e delle misure di sicurezza indicate dal citato Regolamento, nonché delle misure di sicurezza che successivamente verranno indicate in aggiornamento a quelle ivi previste.

La Persona Autorizzata si impegna a mantenere un diligente obbligo di riservatezza rispetto a tutte le informazioni apprese durante lo svolgimento dei compiti ad essa assegnati, anche successivamente alla cessazione del rapporto di lavoro/collaborazione.

La Persona Autorizzata dovrà, inoltre, rispettare le istruzioni impartite dal Titolare. In particolare, dovrà:

➢ trattare i Dati Personali nella misura necessaria e sufficiente alle finalità proprie della banca dati nella quale essi vengono inseriti e delle attività che sono affidate alla Persona Autorizzata;

➢ adottare, nel Trattamento dei dati, tutte le misure di sicurezza che siano indicate, oggi o in futuro, dal Titolare; in particolare, dovrà fare quanto di seguito precisato:

a. per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su Strumenti Aziendale o Strumenti Personali altrui e/o di lasciare aperto il sistema operativo con la propria password inserita, in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare Trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del Trattamento;
b. modificare il proprio codice di accesso personale ogni 3 mesi, nonché provvedere a modificare la password dopo il primo utilizzo;
c. non comunicare o rendere conoscibile a terzi il proprio codice di accesso e/o consentire a terzi di accedere ai dati senza darne preventiva comunicazione al Titolare;
d. non lasciare incustodito e accessibile lo Strumento Aziendale e/o Strumento Personale durante una sessione di Trattamento;
e. trattare i soli dati la cui conoscenza sia necessaria e sufficiente per lo svolgimento delle operazioni da effettuare, nel rispetto del profilo di autorizzazione attribuito;
f. conservare gli Strumenti Aziendali e/o supporti cartacei contenenti dati personali in modo da evitare che detti strumenti siano accessibili a persone non autorizzate al Trattamento dei dati medesimi. Gli Strumenti Aziendali devono, quindi, essere custoditi con diligenza e cura affinché agli stessi non accedano soggetti non autorizzati dal Titolare. Salva autorizzazione per gli Strumenti Personali nei modi previsti dalla Policy sugli strumenti IT, la Persona Autorizzata deve trattare i Dati Personali esclusivamente mediante Strumenti Aziendali;
g. con specifico riferimento agli atti e documenti cartacei contenenti Dati Personali ed alle loro copie, restituire gli stessi al termine delle operazioni affidate, senza mantenerne copia; quando tali atti e i documenti contengono Dati Particolari o Dati Giudiziari e sono affidati alla Persona Autorizzata per lo svolgimento dei relativi compiti, quest'ultima deve controllare e custodire i medesimi atti e documenti con diligenza e cura fino alla restituzione, in maniera che ad essi non accedano persone prive di autorizzazione, e deve restituirli al termine delle operazioni affidategli;
h. non effettuare copie di Dati Personali su Device Mobili, a meno di espressa autorizzazione del Titolare;
i. dare immediata comunicazione al Titolare nel caso si constati o si sospetti un incidente di sicurezza attraverso la Procedura per la gestione dei Data Breach.

➢ segnalare al Titolare eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle predette misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di Trattamento non consentito o non conforme alle finalità della raccolta;

➢ effettuare la comunicazione e la diffusione dei dati esclusivamente e rispettivamente nei confronti dei soggetti indicati dal Titolare, secondo le modalità stabilite dai medesimi, in particolare per quanto riguarda l'eventuale comunicazione di categorie particolari di dati a colleghi e/o consulenti (quali dati relativi alla salute contenuti in referti o altra documentazione medica) che non devono essere associati ai Dati Personali degli interessati stessi;

➢ mantenere, salvo quanto precisato al punto precedente, la massima riservatezza sui Dati Personali, dei quali venga a conoscenza nello svolgimento dell'incarico, per tutta la durata del medesimo ed anche successivamente al termine di esso;

- svolgere, in ogni caso, il Trattamento dei Dati Personali per le finalità e secondo le modalità stabilite, anche in futuro, dal Titolare e, comunque, in modo lecito e secondo correttezza;
- fornire al Titolare, a semplice richiesta e secondo le modalità indicate da questa, tutte le informazioni relative all'attività svolta, al fine di consentire loro di svolgere efficacemente la propria attività di controllo;
- in generale, prestare la più ampia e completa collaborazione al Titolare, al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente.

Ulteriori istruzioni possono essere fornite dal Titolare e possono essere modificate in conformità con le modifiche della normativa vigente.
Per qualsiasi ulteriore aspetto, si rimanda al Regolamento in materia di trattamento dati adottato dall'Ente.
Il titolare del trattamento comunica con la presente che la mancata osservanza di tali istruzioni può far sorgere in capo all'incaricato responsabilità penale per la mancata adozione delle misure minime di sicurezza, responsabilità civile nei confronti di terzi che venissero danneggiati dalla perdita, distruzione e utilizzazione illecita dei dati e responsabilità contrattuale nei confronti dell'Ente.
La presente autorizzazione ha efficacia fino alla risoluzione del rapporto di lavoro per qualsiasi causa oppure fino a modifica o revoca da parte dell'Ente.

Il/la sottoscritto/a prende atto e accetta quanto previsto nella presente assegnazione e dalla normativa vigente ed assume la qualifica di Persona Autorizzata.

Dovera (CR), lì_____

Il Titolare

_____

Per presa visione e accettazione della nomina

_____

Alleg. 2

AUTORIZZAZIONE AL TRATTAMENTO DEI DATI PERSONALI

Egregio/a Sig./Sig.ra _____

Premesso che lei è dipendente del **Comune di Dovera** avente sede in Piazza XXV Aprile, 1 - 26010 Dovera (CR) con la mansione di _____.

Premesso che le attività a lei assegnate comportano il trattamento di dati personali e di dati particolari come definiti all'Art. 4 e all'Art. 9 del Regolamento Europeo 679/2016;

Premesso che l'attività di trattamento dei dati è disciplinata dal Regolamento UE 679/2016 e dalla disciplina vigente;

Premesso che per effetto del Regolamento Europeo UE 679/2016 il Titolare del Trattamento ha l'obbligo di adottare specifiche misure organizzative e di impartire istruzioni a tutti coloro che sono stati autorizzati al trattamento dei dati personali (Artt. 5, 24, 29 e 32).

Tutto ciò premesso

Il Comune, nella persona del Sindaco pro tempore, la autorizza al trattamento dei dati personali. Il trattamento dei dati è consentito al solo ed esclusivo fine di svolgere le mansioni a lei assegnate. Ogni altro tipo di trattamento di dati personali non è consentito. A tal fine lei è autorizzato ad utilizzare la strumentazione informatica e non messa a sua disposizione nelle modalità e in ottemperanza alla presente scrittura, al Regolamento Privacy, alle istruzioni ricevute e alle disposizioni vigenti.
Nell'espletamento delle sue mansioni lavorative lei ha l'obbligo di trattare i dati anche particolari, tra cui quelli relativi alla salute, e tutti i dati personali di cui viene a conoscenza in modo lecito e secondo correttezza, mantenendo assoluto riserbo. È fatto assoluto divieto comunicare, diffondere, utilizzare i dati personali provenienti dalle banche dati e dagli archivi in assenza di autorizzazione del titolare e comunque nei casi non consentiti dalla legge.

Nello specifico lei è autorizzato ad accedere ai dati, conservati sia in formato elettronico che cartaceo, alle seguenti cartelle presenti sul server

ad utilizzare i seguenti software/applicativi

limitatamente alle informazioni previste dal suo profilo e autorizzate dal Titolare del Trattamento.

Lei può accedere alle cartelle e utilizzare i suddetti gestionali/applicativi con le credenziali che le sono state fornite. Le stesse sono strettamente personali e non possono essere comunicate a terzi. Qualsiasi operazione effettuata attraverso

l'inserimento di credenziali identificate dal sistema informatico di riconoscimento viene ricondotta al titolare delle medesime credenziali, indipendentemente dalla postazione di lavoro utilizzata, salvo che lo stesso titolare delle credenziali non fornisca prova contraria. L'elenco degli accessi viene conservato dal sistema informatico per un periodo non inferiore ai 6 (sei) mesi e non superiore ai 12 (dodici) mesi e può essere consultato dal Titolare del Trattamento in caso di necessità e motivi di sicurezza ovvero per motivi di pubblico interesse o connessi all'esercizio di pubblici poteri.

Le è fatto altresì divieto comunicare agli altri incaricati ed a terzi, anche in modo indiretto, le proprie credenziali di autenticazione e le proprie password di accesso ai dispositivi aziendali.

UTILIZZO DELL'ACCOUNT ISTITUZIONALE

Ai fini delle mansioni a lei attribuite, è autorizzato a utilizzare i seguenti account

Ad uso esclusivo
Ad uso condiviso

Premettendo che i soggetti esterni possono attribuire carattere istituzionale alla corrispondenza ricevuta attraverso suddetti account, si ribadisce che per l'utilizzo degli stessi dovrà tenere in debito conto le istruzioni impartite dal Titolare nonché le cautele espresse nella Policy dell'Ente.

ISTRUZIONI PER GLI INCARICATI

La Persona Autorizzata dovrà effettuare il Trattamento dei dati nel rispetto della normativa vigente e delle misure di sicurezza indicate dal citato Regolamento, nonché delle misure di sicurezza che successivamente verranno indicate in aggiornamento a quelle ivi previste.

La Persona Autorizzata si impegna a mantenere un diligente obbligo di riservatezza rispetto a tutte le informazioni apprese durante lo svolgimento dei compiti ad essa assegnati, anche successivamente alla cessazione del rapporto di lavoro/collaborazione.

La Persona Autorizzata dovrà, inoltre, rispettare le istruzioni impartite dal Titolare. In particolare, dovrà:

- trattare i Dati Personali nella misura necessaria e sufficiente alle finalità proprie della banca dati nella quale essi vengono inseriti e delle attività che sono affidate alla Persona Autorizzata;
- adottare, nel Trattamento dei dati, tutte le misure di sicurezza che siano indicate, oggi o in futuro, dal Titolare; in particolare, dovrà fare quanto di seguito precisato:

a. per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su Strumenti Aziendale o Strumenti Personali altrui e/o di lasciare aperto il sistema operativo con la propria password inserita, in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare Trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del Trattamento;
b. modificare il proprio codice di accesso personale ogni 3 mesi, nonché provvedere a modificare la password dopo il primo utilizzo;

c. non comunicare o rendere conoscibile a terzi il proprio codice di accesso e/o consentire a terzi di accedere ai dati senza darne preventiva comunicazione al Titolare;
d. non lasciare incustodito e accessibile lo Strumento Aziendale e/o Strumento Personale durante una sessione di Trattamento;
e. trattare i soli dati la cui conoscenza sia necessaria e sufficiente per lo svolgimento delle operazioni da effettuare, nel rispetto del profilo di autorizzazione attribuito;
f. conservare gli Strumenti Aziendali e/o supporti cartacei contenenti dati personali in modo da evitare che detti strumenti siano accessibili a persone non autorizzate al Trattamento dei dati medesimi. Gli Strumenti Aziendali devono, quindi, essere custoditi con diligenza e cura affinché agli stessi non accedano soggetti non autorizzati dal Titolare. Salva autorizzazione per gli Strumenti Personali nei modi previsti dalla Policy sugli strumenti IT, la Persona Autorizzata deve trattare i Dati Personali esclusivamente mediante Strumenti Aziendali;
g. con specifico riferimento agli atti e documenti cartacei contenenti Dati Personali ed alle loro copie, restituire gli stessi al termine delle operazioni affidate, senza mantenerne copia; quando tali atti e i documenti contengono Dati Particolari o Dati Giudiziari e sono affidati alla Persona Autorizzata per lo svolgimento dei relativi compiti, quest'ultima deve controllare e custodire i medesimi atti e documenti con diligenza e cura fino alla restituzione, in maniera che ad essi non accedano persone prive di autorizzazione, e deve restituirli al termine delle operazioni affidategli;
h. non effettuare copie di Dati Personali su Device Mobili, a meno di espressa autorizzazione del Titolare;
i. dare immediata comunicazione al Titolare nel caso si constati o si sospetti un incidente di sicurezza attraverso la Procedura per la gestione dei Data Breach.

➢ segnalare al Titolare eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle predette misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di Trattamento non consentito o non conforme alle finalità della raccolta;

➢ effettuare la comunicazione e la diffusione dei dati esclusivamente e rispettivamente nei confronti dei soggetti indicati dal Titolare, secondo le modalità stabilite dai medesimi, in particolare per quanto riguarda l'eventuale comunicazione di categorie particolari di dati a colleghi e/o consulenti (quali dati relativi alla salute contenuti in referti o altra documentazione medica) che non devono essere associati ai Dati Personali degli interessati stessi;

➢ mantenere, salvo quanto precisato al punto precedente, la massima riservatezza sui Dati Personali, dei quali venga a conoscenza nello svolgimento dell'incarico, per tutta la durata del medesimo ed anche successivamente al termine di esso;

➢ svolgere, in ogni caso, il Trattamento dei Dati Personali per le finalità e secondo le modalità stabilite, anche in futuro, dal Titolare e, comunque, in modo lecito e secondo correttezza;

➢ fornire al Titolare, a semplice richiesta e secondo le modalità indicate da questa, tutte le informazioni relative all'attività svolta, al fine di consentire loro di svolgere efficacemente la propria attività di controllo;

➢ in generale, prestare la più ampia e completa collaborazione al Titolare, al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente.

Ulteriori istruzioni possono essere fornite dal Titolare e possono essere modificate in conformità con le modifiche della normativa vigente.

Per qualsiasi ulteriore aspetto, si rimanda al Regolamento in materia di trattamento dati adottato dall'Ente.
Il titolare del trattamento comunica con la presente che la mancata osservanza di tali istruzioni può far sorgere in capo all'incaricato responsabilità penale per la mancata adozione delle misure minime di sicurezza, responsabilità civile nei confronti di terzi che venissero danneggiati dalla perdita, distruzione e utilizzazione illecita dei dati e responsabilità contrattuale nei confronti dell'Ente.
La presente autorizzazione ha efficacia fino alla risoluzione del rapporto di lavoro per qualsiasi causa oppure fino a modifica o revoca da parte dell'Ente.

Il/la sottoscritto/a prende atto e accetta quanto previsto nella presente assegnazione e dalla normativa vigente ed assume la qualifica di Persona Autorizzata.

Dovera (CR), lì_____

Il Titolare

_____

Per presa visione e accettazione della nomina

_____

Per presa visione, comprensione e accettazione di quanto espresso

NOME E COGNOME	Firma