Ù

MANUALE PRIVACY

Comitato Paritetico Territoriale della Provincia di Salerno

Per la protezione dei dati personali ai sensi del Regolamento (UE) 2016/679 - (GDPR)

1. PREMESSA

Il presente Documento Unico Privacy è stato redatto in conformità al Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio (GDPR), in particolare sulla base di quanto disposto dall'art. 32 in merito alla *valutazione dei rischi nel trattamento dati e alle misure tecniche organizzative adeguate per garantire un livello adeguato di sicurezza*.

È rivolto agli utenti dell'ente bilaterale del settore edile, Comitato Paritetico Territoriale della Provincia di Salerno, da ora in avanti denominato brevemente ENTE o CPT.

All'Ente, in qualità di *Titolare* del trattamento dei dati personali, competono le decisioni in ordine alle finalità ed alle modalità del trattamento degli stessi dati, compreso il profilo della sicurezza e della prevenzione da un potenziale Data Breach (violazione dei dati).

In considerazione di quanto sopra, gli obiettivi primari del presente Documento sono i seguenti:

- migliorare la consapevolezza dei rischi insiti nel trattamento dei dati con l'ausilio di strumenti elettronici, con particolare riferimento alla gestione e all'utilizzo del sistema informativo ed effettuare una valutazione di rischio sui trattamenti dei dati personali dell'Ente;
- individuare e definire adeguate misure tecniche ed organizzative finalizzate alla salvaguardia, alla corretta gestione e al corretto utilizzo del patrimonio informativo aziendale;
- adottare idonei presidi di controllo al fine di contenere i rischi, prevenendo le possibili situazioni di pericolo;
- fornire adeguate istruzioni comportamentali e procedurali ai soggetti coinvolti nella gestione dei singoli trattamenti.

Per il raggiungimento dei suddetti obiettivi l'Ente pone in essere, fra l'altro, le seguenti attività:

- censimento dei trattamenti effettuati e delle banche dati gestite dagli incaricati, al fine di individuare le diverse tipologie di dati trattati, i rischi potenziali e le conseguenti misure di sicurezza (art. 32 Reg.);
- predisposizione di un Documento Unico Privacy per il trattamento dei dati personali con cui vengono fatte proprie le regole deontologiche e le misure minime di sicurezza previste dal nuovo Regolamento (UE) 2016/679, in materia di protezione dei dati personali;
- predisposizione di un apposito Registro delle attività del trattamento (art. 30 Reg.) dove verranno riportate tutte le informazioni relative a:
- nome del titolare (o del responsabile del trattamento o del titolare per cui si agisce);
- descrizione delle attività effettuate dal titolare (o per conto del titolare);
- finalità del trattamento dei dati;

- base giuridica del trattamento;
- categorie di dati;
- destinatari dei dati;
- misure di sicurezza adottate;
- termini per la cancellazione dei dati;
- destinatati UE e Extra UE

Le attività di cui sopra hanno portato all'acquisizione e all'aggiornamento delle seguenti informazioni, trattate in modo approfondito nei successivi paragrafi del presente Documento:

- elenco dei trattamenti di dati personali;
- distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- analisi e valutazione dei rischi che incombono sui dati;
- misure da adottare per garantire l'integrità e la disponibilità dei dati e la protezione delle aree e dei locali;
- descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- previsione di interventi formativi degli incaricati del trattamento;
- descrizione dei criteri da adottare per garantire l'adozione delle misure di sicurezza in caso di trattamento di dati personali affidati all'esterno della struttura del titolare.

2. DEFINIZIONI

Trattamento: qualsiasi operazione o insieme di operazioni compiute con o senza l'analisi di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, la conservazione, l'uso, la comunicazione mediante diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determinano le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi del trattamento di dati personali 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 dai paesi degli Stati membri.

Responsabile del trattamento: la persona fisica o giuridica l'autorità pubblica o altro organismo che tratta dati personali per conto del titolare del trattamento**.** Il Regolamento fissa in modo dettagliato le caratteristiche dell'atto con cui il Titolare del trattamento designa un Responsabile del trattamento, attraverso la stipula di un contratto o altro atto giuridico che regoli la materia disciplinata e la durata del trattamento, la natura e le finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare.
Può essere nominato un responsabile interno mediante lettera di incarico.
Nei casi in cui vi siano servizi di ***outsourcing,*** l'outsourcer assume sempre la veste di

Responsabile esterno e il trattamento dei dati da esso effettuato deve essere regolato da un contratto (anche il contratto di servizi stesso).

Incaricato: il dipendente che è coinvolto materialmente nel trattamento dei dati (ad es. amministrazione del personale) e incaricato attraverso un'apposita ***lettera di incarico***.

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 una o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Es. Dati personali

- codice fiscale e altri numeri di identificazione personale
- nominativo, indirizzo o altri elementi di identificazione personale
- dati relativi alla famiglia e a situazioni personali
- dati bancari o postali
- carta identità
- istruzione
- formazione
- dati relativi ai familiari, anche minori, del lavoratore iscritto

Dati Particolari (ex sensibili): i 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 biomedici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
Es. Dati particolari

- adesione ad un sindacato
- stato di salute
- origine razziale ed etnica
- convinzioni religiose filosofiche o di altro genere
- opinioni politiche
- organizzazioni a carattere religioso, filosofico, politico o sindacale

Responsabile della Protezione dei Dati (RDP ovvero DPO se si usa l'acronimo inglese Data Protection Officer): è un professionista con conoscenze specialistiche della normativa e della prassi designato dal titolare e/o dal responsabile del trattamento il quale garantisce standard di sicurezza adeguati. Può anche essere un dipendente del titolare o del responsabile del trattamento ovvero assolvere i suoi compiti in base a un contratto di servizi quale esterno. Il titolare o il responsabile del trattamento pubblica i dati di contatto del DPO e li comunica all'Autorità di controllo. Rientrano tra i suoi compiti la sensibilizzazione e la formazione del personale e la sorveglianza della valutazione d'impatto. In particolar modo:

- informare e fornire consulenza al titolare e al responsabile del trattamento in merito agli obblighi derivanti dal Regolamento o dalle altre disposizioni legislative interne o europee in materia di protezione dati;
- sorvegliare l'osservanza del Regolamento da parte del titolare e del responsabile del trattamento in tutte le sue parti, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa al trattamento;

- fornire su richiesta pareri in merito alla valutazione d'impatto e sorvegliarne lo svolgimento;
- cooperare con l'autorità di controllo fungendo, tra le altre cose, da punto di contatto per questioni connesse al trattamento effettuando consultazioni di ogni tipo, con particolare riguardo e attenzione ad un'eventuale attività di consultazione preventiva.

È un soggetto indipendente che svolge un ruolo anche di *mediatore* nei rapporti tra gli interessati, i responsabili, il titolare e fa da tramite tra quest'ultimo e l'Autorità di controllo. Supporta tutti i soggetti che all'interno dell'Ente si occupano di privacy e hanno a che fare con il trattamento dei dati.

Modalità Del Trattamento: il regolamento sancisce che il trattamento deve sempre ispirarsi ai principi di liceità, correttezza, trasparenza, pertinenza, compatibilità con le finalità espresse con gli scopi dichiarati, minimizzazione, proporzionalità, limitazione alla conservazione, sicurezza e integrità

Data Breach (o violazione dei dati): tutti i titolari dovranno notificare all'autorità di controllo le ***violazioni dei dati*** personali di cui vengono a conoscenza entro le 72 ore e comunque senza "ingiustificato ritardo". La notifica dovrà avvenire solo se i titolari ritengano che dalla violazione derivino rischi per i diritti e le libertà dell'interessato. Nella logica del Regolamento, ispirato al principio della responsabilizzazione (*accountability*) di titolari e responsabili ovverosia sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento, la notifica all'Autorità dell'avvenuta violazione non è obbligatoria in quanto è subordinata alla valutazione del rischio per gli interessati.
Tale valutazione spetta al titolare. E' altresì sancito che laddove la probabilità del rischio è elevata si dovrà informare della violazione anche l'interessato sempre "senza giustificato ritardo".

Liceità del Trattamento – Basi Giuridiche del Trattamento dei Dati: il trattamento dei dati è lecito se ricorre almeno una delle seguenti condizioni:

- l'interessato ha prestato il consenso
- il trattamento è necessario all'esecuzione di un contratto
- il trattamento è necessario per adempiere ad un obbligo di legge
- il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato
- il trattamento è necessario per l'esecuzione di un compito di interesse pubblico
- il trattamento è necessario per il perseguimento di un legittimo interesse del titolare

Consenso: come per la previgente normativa, il consenso deve essere libero, specifico, informato e inequivocabile e non è ammesso il consenso tacito o presunto. Deve essere manifestato attraverso "dichiarazione o azione positiva inequivocabile". Il Regolamento prevede che il consenso deve essere esplicito per i dati particolari (ex sensibili) cosi come per il consenso basato su trattamenti automatizzati come ad esempio la profilazione. Il titolare deve essere sempre in grado di dimostrare che l'interessato ha prestato il proprio consenso a uno specifico trattamento. Per questo è richiesto che le informazioni e le comunicazioni relative al trattamento dei dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro. Trova ingresso il principio che il consenso dei minori

è valido a partire dai 16 anni e prima di tale età il consenso è raccolto dai genitori o da chi ne fa le veci.

Informativa: il Regolamento, diversamente dal Codice, detta le caratteristiche dell'informativa in maniera più dettagliata nel senso che deve avere una forma coincisa, trasparente, intelligibile per l'interessato e facilmente accessibile. E' necessario utilizzare un linguaggio chiaro e semplice e per i minori prevedere idonee informative. Generalmente l'informativa richiede la forma scritta e preferibilmente in formato elettronico ma sono ammessi anche altri mezzi, purché possa esserne data prova.

Contenuti dell'informativa: l'informativa deve:

- specificare i dati di contatto del Responsabile del trattamento e del RPD-DPO (ove esistente):
- indicare la base giuridica del trattamento;
- indicare qual è l'interesse legittimo del titolare;
- trasferimento dei dati personali in Paesi terzi e attraverso quali strumenti;
- periodo di conservazione dei dati;
- diritto di presentare ricorso all'autorità di controllo.

Tempi dell'informativa: se i dati non sono stati raccolti direttamente dall'interessato l'informativa deve essere fornita entro 1 mese dalla raccolta altrimenti al momento della comunicazione dei dati.

Diritti dell'interessato: il legislatore comunitario ha introdotto nuovi diritti in capo all'interessato:

- diritto di accesso dell'interessato al trattamento dei propri dati;
- diritto di rettifica (senza ingiustificato ritardo);
- diritto all'oblio o diritto alla cancellazione dei dati;
- diritto di limitazione;
- diritto alla portabilità dei dati (da un titolare ad un altro);
- diritto di opposizione (al trattamento dei propri dati)

3. TRATTAMENTI DEI DATI SVOLTI DAL COMITATO PARITETICO TERRITORIALE DELLA PROVINCIA DI SALERNO

3.1 Natura dei Dati Trattati dal Comitato Paritetico Territoriale della Provincia di Salerno

L'ambito di applicazione del presente documento riguarda i trattamenti dei **dati personali** effettuati dal CPT della Provincia di Salerno; in particolare il CPT può trattare sia i dati personali dei propri **dipendenti**, che quelli degli **operai iscritti** e dei loro familiari, dei **rappresentanti d'impresa**, oltre ai dati di eventuali **altri utenti** (dati di terzi collaboratori, dei fornitori etc.).

3.2 Tipologia dei dati trattati dall'Ente e modalità di trattamento

Il CPT della Provincia di Salerno tratta:

- ✓ **dati anagrafici**: nominativo, indirizzo ed altri elementi di identificazione personale, dati bancari e postali, e-mail, cellulare,
- ✓ **dati familiari**: i dati relativi ai componenti della famiglia e a situazioni personali.
- ✓ **dati particolari**: origine razziale ed etnica, stato di salute ed adesione ad un sindacato.
- ✓ Ogni altro dato utile o indispensabile per la applicazione della contrattazione collettiva di settore.
  Non è possibile, inoltre, escludere a priori il trattamento di dati "*giudiziari*" nel corso dell'attività di recupero crediti degli Enti.

Il CPT della Provincia di Salerno esegue i trattamenti, mediante la creazione di apposite banche dati ed archivi, gestite con **strumenti elettronici**, attraverso il proprio sistema informativo e/o attraverso strumenti tradizionali, tramite i propri **archivi cartacei.**

3.3 Fonte di Raccolta Dati degli interessati

I dati sono raccolti secondo le seguenti modalità (e previa contestuale informativa da fornire agli interessati (i lavoratori), salvo fornirla entro un mese dalla raccolta dei dati quando questa avviene presso l'impresa):

- **dall'interessato**, tramite, contratti di lavoro, moduli d'iscrizione (disponibili anche su Web), denunce mensili, dichiarazioni, domande per prestazioni assistenziali extracontrattuali e deleghe sindacali;
- **da soggetti diversi dall'interessato**, quali ad esempio consulenti del lavoro, associazioni sindacali (con apposita delega)

3.4 Finalità dei Trattamenti

I trattamenti dei dati hanno finalità differenti in base al rapporto con cui Il CPT della Provincia di Salerno intrattiene con gli utenti , come descritto a seguire e nelle Informative appositamente redatte.

DATI dei DIPENDENTI/AMMINISTRATORI
la finalità del trattamento è quella di consentire al Titolare la gestione ed esecuzione del rapporto di lavoro. Tra gli obblighi contrattuali e di legge maggiormente significativi rileviamo, non a titolo esaustivo:

- costituzione del rapporto di lavoro;
- adempimento degli obblighi retributivi, fiscali, previdenziali, assistenziali e contabili, relativamente al personale in servizio o in pensione;
- adempimento degli specifici obblighi o svolgimento dei compiti previsti dalla normativa in materia di salute e sicurezza sul luogo di lavoro, nonché in materia sindacale;
- esercizio e godimento (individuale) dei diritti e dei vantaggi connessi al lavoro;
- la riscossione dei contributi per la previdenza complementare;
- l'attuazione dei contratti ed accordi collettivi di riferimento

DATI di SOGGETTI TERZI
la finalità del trattamento è quella di dare esecuzione a contratti con essi stipulati e relativi impegni (es. Fornitori); dare esecuzioni a collaborazioni esterne per l'adempimento degli

obblighi di legge (es. Consulenti del Lavoro) etc.

3.5 Base giuridica dei Trattamento

l regolamento UE conferma che ogni trattamento svolto dal Titolare, deve trovare fondamento in un'idonea base giuridica; i fondamenti di liceità del trattamento sono indicati all'art. 6 del regolamento stesso.
La base giuridica che giustifica la maggior parte dei trattamenti svolti dal CPT della Provincia di Salerno è l'adempimento di misure precontrattuali e obblighi contrattuali (es. verso i dipendenti, i lavoratori iscritti ai corsi, i fornitori), inoltre, in relazione ad eventuali servizi opzionali offerti dal CPT della Provincia di Salerno agli interessati, la base giuridica del trattamento può essere il libero consenso, che viene richiesto all'interessato in modo chiaro ed inequivocabile nella modulistica specifica e che è sempre revocabile.
Infine, il legittimo interesse del titolare è la base giuridica utilizzata per la videosorveglianza.

Le tipologie, le modalità dei trattamenti, le basi giuridiche, gli interessati, saranno esemplificate nell'apposito ***Registro dei Trattamenti***.

Il CPT della Provincia di Salerno della provincia di Salerno fornisce per ogni categoria di interessati, un'apposita ***Informativa*** sul Trattamento dei Dati, presente anche sul sito internet.

3.6 Designazione e attività degli incaricati

Ogni operatore che agisce sotto l'autorità del Titolare o del Responsabile è ***incaricato*** al trattamento dei dati derivanti dall'espletamento dei compiti e delle funzioni ad esso attribuiti dal contratto di lavoro e dal profilo abilitativo assegnato, in conseguenza della sua preposizione ad una determinata unità operativa, risultante dalla relativa lettera di incarico.

Gli incaricati, nel trattare i dati personali, dovranno operare garantendo **la massima riservatezza** delle informazioni di cui vengono in possesso. Dovranno considerare tutti i dati personali come confidenziali e, di norma, soggetti al segreto d'ufficio, fatta eccezione per i soli dati anonimi, generalmente trattati per elaborazioni statistiche, e per quelli acquisibili da chiunque perché contenuti in atti, liste ed elenchi pubblici (che non rilevano ai fini del Regolamento UE).
Le procedure di lavoro, le prassi operative e la condotta tenuta nello svolgimento delle operazioni di trattamento, dovranno mirare ad evitare che:

- i dati personali siano soggetti a rischi di distruzione o perdita anche accidentale;
- i dati possano accedere persone non autorizzate;
- vengano svolte operazioni di trattamento non consentite o non conformi ai fini per i quali i dati stessi sono stati raccolti.

Deve, quindi, sempre garantirsi **l'integrità del dato**, la sua **disponibilità** e la sua **confidenzialità**.

Gli incaricati dovranno perciò operare con la massima diligenza ed attenzione in tutte le fasi di trattamento: dalla esatta acquisizione dei dati, all'eventuale loro aggiornamento; così per la conservazione, la custodia ed eventuale cancellazione o distruzione.

Gli incaricati non potranno pertanto eseguire operazioni di trattamento per fini non previsti tra i compiti loro assegnati e comunque riferiti alle disposizioni e regolamenti vigenti nella CPT della Provincia di Salerno.

In seguito a quanto emerso dall'effettuazione del censimento dei trattamenti di dati personali e dall'analisi dei rischi, si stabilisce quanto segue:

- i dati particolari (ex sensibili) circa le ***adesioni ad attività formative, le richieste delle Imprese o loro rappresentanti, i risultati delle visite in cantiere*** **potranno essere trattati esclusivamente dai soggetti all'uopo individuati;**
- ogni altro incaricato al trattamento di dati particolari (ex sensibili), diverso dai soggetti indicati al precedente punto dovrà ricevere specifiche indicazioni scritte o verbali che integrano quelle generali di cui al presente regolamento;
- gli incaricati che svolgono operazioni di trattamento di dati particolari (ex sensibili), utilizzando elaboratori, sono autorizzati altresì all'accesso agli strumenti abilitati per tali trattamenti, all'accesso ai locali in cui vengono svolte tali lavorazioni ed alle operazioni di trattamento, attenendosi alle norme di sicurezza stabilite dall'Ente per tali trattamenti.

Gli incaricati, dovranno attenersi scrupolosamente alle ***Istruzioni*** impartite dal Titolare e descritte nel presente documento.

3.7 Destinatari della Comunicazione dei dati

I dati trattati possono essere comunicati, esclusivamente per la realizzazione delle finalità sopra specificate, ai seguenti soggetti:

- Pubbliche Amministrazioni che richiedano informazioni al CPT della Provincia di Salerno della provincia di Salerno in ottemperanza ad obblighi di legge
- Enti di previdenza come Inps, Inail e Fondi previdenza complementare
- Istituti bancari e finanziari che intrattengono rapporti con Il CPT della Provincia di Salerno della provincia di Salerno
- Società di servizio per la realizzazione delle finalità del CPT della Provincia di Salerno della provincia di Salerno
- Altri CPT o Enti Unici e loro organismi di coordinamento
- Enti paritetici di categoria
- Associazioni imprenditoriali e sindacali
- Società di revisione contabile
- Legali e altri consulenti esterni del CPT della Provincia di Salerno della provincia di Salerno
- componenti del Comitato di gestione (amministratori) e del Collegio sindacale
- sindacato di appartenenza
- Società assicurative
- personale dipendente del CPT della Provincia di Salerno della provincia di Salerno
- società di vigilanza e controllo.

3.9 Comunicazione e divulgazione dei dati ai Responsabili Esterni del Trattamento

Qualora il trattamento dei dati debba essere effettuato da terzi, per conto del titolare, quest'ultimo deve avere tutte le garanzie che il trattamento si svolga secondo i requisiti del Regolamento e garantisca la tutela degli interessati.
I trattamenti da parte di un eventuale **Responsabile Esterno** sono disciplinati mediante un contratto (anche lo stesso contratto di servizi) che prevede che il soggetto cui le attività sono affidate si impegna a (art. 32 del Reg.):

- trattare i dati personali soltanto su istruzione documentata del titolare del trattamento anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento dovrà informare titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
- garantire che le persone autorizzate al trattamento dei dati personali si siano a loro volta impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- adottare tutte le misure richieste ai sensi dell'art. 32;
- rispettare le condizioni di cui ai paragrafi 2 e 4 per ricorrere ad un altro responsabile del trattamento;
- assistere il titolare del trattamento, tenendo conto della natura del trattamento, con misure tecnico organizzative adeguate, nella misura di cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;
- assistere il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della misura del trattamento;
- cancellare o restituire, su scelta del titolare del trattamento tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;
- mettere a disposizione del titolare del trattamento di tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato. Si impegna ad informare senza ritardo il titolare del trattamento qualora, a suo parere, un'istruzione violi il Regolamento o altre disposizioni, nazionali o dell'Unione, relativa alla protezione dei dati.

Sono previste verifiche periodiche da parte del Titolare presso i Responsabili esterni all'Ente in merito al rispetto delle disposizioni in materia di trattamento, compreso il profilo della sicurezza.

Gli operatori esterni incaricati dell'assistenza tecnica (ad es. società informatica) ai sistemi di elaborazione dei dati, sono identificati mediante ***atto di nomina*** (anche contratto di servizi) che deve indicare, come sopra riportato, tutti gli obblighi cui è soggetto quale Responsabile esterno.

Si rinvia al ***Registro del Trattamento*** dei dati personali per l'individuazione dei nominativi dei terzi destinatari della comunicazione dei dati e dei Responsabili Esterni, trattati dal *CPT della Provincia di Salerno*.

3.10 Responsabile del trattamento interno

Il CPT della Provincia di Salerno ha individuato all'interno della propria organizzazione un Responsabile interno del Trattamento che, come previsto al par. 2 "Definizioni", è stato formalmente incaricato mediante apposito atto di nomina.

4. DESCRIZIONE DEI LUOGHI DI LAVORO E MODALITA' DI ACCESSO AI DATI

6.1 Luoghi di lavoro e misure logistiche

L'ingresso principale alla sede del CPT della Provincia di Salerno si trova in Via Cerzone 1 e consiste in un'anticamera da cui si accede agli uffici ed alle aule.

Presenza dei seguenti dispositivi di **rilevazione passiva**

Dispositivo	Si	No	% di locali
Rilevatore di fumo	X		100
Rilevatore d'incendio	X		100
Rilevatore d'allagamento		X	100

Presenza dei seguenti dispositivi di **rilevazione attiva**

Dispositivo	Si	No	% di locali
Impianti fissi soppressione incendio		X	100
Condizionamento ambiente e segnalazione anomalie	X		100

Presenza dei seguenti **dispositivi infrastrutturali**

Dispositivo	Si	No	% di locali
Armadi ignifughi e stagni	X		20
Quadro elettrico chiuso a chiave	X		20
Armadio per i dispositivi di fonia e dati chiuso a chiave	X		
Estintori	X		100

Presenza dei seguenti **dispositivi di controllo accessi fisici**

Dispositivo	Si	No	% di locali

Porta di accesso unica con chiave unica	X		100
Controllo accessi con chiave ai locali in cui sono dislocati server o apparati tecnici	X		100
Impianto anti-intrusione	X		100
Videosorveglianza		X	

6.2 Schedari e supporti cartacei

Nella sede tutta la documentazione cartacea viene raccolta in archivi, i quali vengono custoditi in armadi chiusi.
L'accesso agli archivi contenti atti e documenti di dati particolari (ex sensibili) viene controllato dal personale incaricato appartenente alla funzione di competenza.

5. NOTIFICA IN CASO DI DATA BREACH

Ai sensi dell'Articolo 33 del GDPR, ovvero in caso di violazione di archivi contenenti dati personali (ma, anche, in caso di smarrimento o furto di una chiavetta, di un hard disk esterno o di un computer portatile) l'Ente titolare deve notificare la suddetta violazione all'autorità di controllo competente (ossia al Garante) **entro 72 ore** dal momento in cui ne è venuto a conoscenza.
La comunicazione deve essere fatta anche a tutti gli utenti/interessati cui i dati si riferiscono, a meno che sia improbabile che quella violazione dell'archivio rappresenti un rischio per i diritti e le libertà delle persone fisiche.
Oltre il termine di 72 ore, tale comunicazione deve essere accompagnata dalle ragioni del ritardo nell'agire in tal senso.
La notifica, in particolare, deve descrivere la natura della violazione, indicando – ove possibile – le categorie e il numero approssimativo dei dati personali violati e degli interessati coinvolti.
Deve, inoltre, contenere il nome e i dati di contatto del responsabile interno del trattamento dell'Ente o di un altro punto di contatto presso cui sia consentito ottenere più informazioni.
Infine, deve descrivere le probabili conseguenze della violazione e le misure adottate, o di cui si propone l'adozione, al fine di porre rimedio alla violazione o di attenuarne i possibili effetti negativi.

Ai sensi dell'Articolo 34, poi, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, l'Ente comunicherà senza indebito ritardo anche all'interessato stesso, consentendogli, in tal modo, di prendere le

precauzioni necessarie.
La comunicazione descriverà la natura della violazione e conterrà le raccomandazioni, per la persona fisica interessata, dirette ad attenuare i potenziali effetti negativi (ad esempio: il suggerimento di cambiare immediatamente le credenziali).
L'Ente si impegna a effettuare tale comunicazione non appena ragionevolmente possibile, in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti.
La comunicazione all'interessato tuttavia **non è richiesta** nei seguenti casi:

- quando il titolare del trattamento ha messo in atto, e applicato ai dati che sono stati oggetto di violazione, tutte le necessarie misure tecniche e organizzative di protezione, comprese quelle destinate a rendere i dati personali incomprensibili ai soggetti non autorizzati (come, ad esempio, la cifratura delle informazioni);
- quando il titolare del trattamento abbia successivamente adottato misure per scongiurare il verificarsi di un rischio elevato per i diritti e le libertà degli interessati;
- quando la comunicazione stessa richiederebbe sforzi sproporzionati e, in tal caso, si può procedere a una comunicazione pubblica o ad altra soluzione analoga, così da informare gli interessati in maniera ugualmente efficace.

6. ISTRUZIONI AGLI INCARICATI PER I TRATTAMENTI SVOLTI CON STRUMENTI ELETTRONICI

I dipendenti, i collaboratori ed in generale tutte le persone autorizzate ad accedere ai dati personali e preposte allo svolgimento delle operazioni di trattamento relativa ai dati, devono ispirarsi a un principio generale di diligenza e correttezza. Ogni utilizzo dei dati in possesso dell'incaricato, diverso da finalità strettamente professionali, è espressamente vietato. Di seguito vengono esposte le regole comportamentali da seguire per evitare e prevenire condotte che anche inconsapevolmente potrebbero compromettere la riservatezza, integrità e la disponibilità dei dati.

INDICAZIONI DI ORDINE GENERALE:

- ✓ Porre molta attenzione sui dati che l'incaricato comunica a soggetti terzi esterni in relazione allo svolgimento delle proprie mansioni:
  - è raccomandabile acquisire sempre richieste formali scritte da parte del soggetto che richiede il dato
  - i dati non possono essere comunicati a terzi soggetti diversi dagli interessati senza una formale delega scritta e verifica dell'identità del soggetto delegato, né in istanze presentate al telefono, né presentandosi personalmente presso gli uffici.
  - gli incaricati non sono, in nessun caso, tenuti a comunicare informazioni, circa i lavoratori e le imprese, richieste telefonicamente.
  - in caso di informazioni richieste al telefono da soggetti che si qualificano come interessati, l'incaricato dovrà identificare l'interlocutore richiedendo dati verificabili nella banca dati

come ad esempio nome e cognome, data di nascita, codice fiscale, ecc., in generale qualsiasi altra informazione riferibile al soggetto.

- qualora, nello svolgimento della propria attività lavorativa, l'incaricato si trovasse nella situazione di dover procedere alla comunicazione o diffusione di dati, oltre i limiti previsti, è invitato a rivolgersi al proprio Responsabile per ricevere le istruzioni del caso.

✓ Non è consentito il trattamento di dati particolari per fini esclusivamente personali anche se non effettuato con elaboratori stabilmente accessibili da altri elaboratori

GESTIONE DEL PC

Ciascun incaricato è responsabile del corretto utilizzo e della custodia degli strumenti elettronici in dotazione (a titolo esemplificativo personal computer, periferiche, lettori di smart card). Si devono adottare le misure di sicurezza per la tutela della riservatezza, consistenti nell'evitare che l'accesso ai dati possa avvenire da parte di soggetti estranei all'organizzazione o non specificamente autorizzati.

✓ Per la gestione della sessione di lavoro sul PC connesso in rete, è necessario che:

- al termine delle ore di servizio, il PC deve essere spento, a meno che non stia svolgendo elaborazioni particolari. In tal caso gli uffici debbono tassativamente essere chiusi a chiave;
- Se l'incaricato si assenta momentaneamente dalla propria postazione deve accertarsi che l'eventuale sessione di lavoro aperta non sia accessibile da altre persone. Pertanto deve chiudere la sessione di lavoro sul PC facendo Logout, oppure in alternativa deve avere attivo un salvaschermo (screen- saver) protetto dalle credenziali di autenticazione; relativamente all'utilizzo dello screen-saver, occorre osservare le seguenti norme:
  - non deve mai essere disattivato;
  - il suo avvio automatico deve essere previsto non oltre i primi 10 minuti di inattività del PC;
  - deve essere messo in funzione manualmente ogni volta che si lascia il PC incustodito ed acceso;

GESTIONE DELLE STAMPE/SUPPORTI CARTACEI

Quando si esegue la stampa di un documento contenente dati personali, in particolare su una stampante condivisa, occorre ritirare tempestivamente i documenti stampati per evitare l'accesso a soggetti non abilitati al trattamento.

GESTIONE DELLE CREDENZIALI DI AUTENTICAZIONE

Tutti gli incaricati, come visto in precedenza, sono dotati di credenziali di autenticazione (nome utente e password). Il trattamento dei dati personali richiede il superamento di una o più procedure di autenticazione, per l'accesso alla rete e/o alle singole applicazioni.
L'adozione ed il corretto utilizzo della combinazione username / password è fondamentale per il corretto utilizzo del PC, in quanto:

- tutela l'utilizzatore ed in generale l'Ente da accessi illeciti, atti di vandalismo e, in generale, violazioni e danneggiamenti del proprio patrimonio informativo;
- tutela l'Incaricato da false imputazioni, garantendo che nessuno possa operare a suo nome e che, con il suo profilo (ossia con le sue user id e password) solo lui possa svolgere determinate azioni;

- è necessario per gestire correttamente gli accessi a risorse condivise.

✓ Per quanto riguarda la username:
  - è composto dal "nome cognome"
  - non può essere mai utilizzato, neanche in momenti diversi, da altri incaricati che non siano l'assegnatario. Pertanto, non è consentito in nessun momento che una persona si connetta al sistema informativo "presentandosi" come se fosse un'altra.

✓ Ciascun incaricato deve scegliere le ***password*** in base ai seguenti criteri:
  - deve essere composta da almeno otto caratteri possibilmente utilizzando lettere minuscole e maiuscole e/o numeri anche in combinazione fra loro;
  - la password non deve comunque contenere riferimenti agevolmente riconducibili all'incaricato come ad esempio il nome o la data di nascita o loro parti;
  - non deve essere uguali alle precedenti;

✓ Per la corretta gestione della password è necessario:
  - almeno ogni 6 mesi è obbligatorio cambiare la password;
  - ogni password ricevuta va modificata al primo utilizzo;
  - non deve essere divulgata e deve essere custodita con la massima diligenza (es evitare di custodire per iscritto la propria password presso la postazione di lavoro);
  - non utilizzare la funzione, offerta da alcuni software, di salvare automaticamente la password per successivi utilizzi delle applicazioni.
  - provvedere all'immediata sostituzione qualora per motivazioni direttamente o indirettamente imputabili all'operare dell'incaricato, la password sia venuta a conoscenza di altre persone;

GESTIONE DI HARDWARE E SOFTWARE

L'installazione di hardware e software, nonché la modifica dei parametri di configurazione, possono essere eseguiti solamente dall'Amministratore di Sistema. Pertanto si raccomanda agli utenti dei PC di rispettare i seguenti divieti:

- non utilizzare sui PC dell'Ente, dispositivi personali, o comunque non aziendali, quali lettori dispositivi di memorizzazione dei dati;
- non è consentito l'uso di programmi diversi da quelli ufficialmente installati nei PC del CPT della Provincia di Salerno né viene consentito agli incaricati di installare autonomamente programmi provenienti dall'esterno, sussistendo, infatti, il grave pericolo di introdurre virus informatici e/o alterare la funzionalità di applicazioni software esistenti. L'inosservanza della presente disposizione espone il CPT della Provincia di Salerno a gravi responsabilità civili; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sui software, che impone la presenza nel sistema di software regolarmente licenziati o comunque liberi e quindi non protetti dal diritto di autore, vengono sanzionate anche penalmente.
- Non installare sistemi per connessione esterne (es modem, wifi); tali connessioni, aggirando i sistemi preposti alla sicurezza della rete aziendale, aumentano sensibilmente i rischi di intrusioni e di attacchi dall'esterno;
- Non modificare i parametri di configurazione del proprio PC senza espressa autorizzazione e senza il supporto di personale tecnico qualificato.
- L'antivirus installato nel PC non deve mai essere disattivato o sostituito con altro antivirus non ufficialmente fornito. Nel caso il programma antivirus installato nel PC riscontri la presenza di

un virus, oppure si sospetti la presenza di un virus non rilevato dal programma antivirus è necessario darne immediatamente segnalazione all'amministratore di sistema.

GESTIONE DELLA POSTA ELETTRONICA

L'utilizzo della posta elettronica interna contribuisce fortemente a rendere la comunicazione tempestiva, efficace ed economica. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. Il rispetto di alcune semplici regole può aiutarci a migliorare ulteriormente l'utilizzo dello strumento:

- la casella di posta personale deve essere mantenuta in ordine, cancellando i messaggi inutili specialmente se contengono allegati ingombranti o se sono stati segnalati dall'antivirus;
- è buona norma evitare i messaggi completamente estranei al rapporto di lavoro o, al limite, alle relazioni tra colleghi; l'incaricato ha il divieto quindi di utilizzare le caselle di posta elettronica dell'Ente per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing list salvo diversa ed esplicita autorizzazione.
- per la trasmissione di file all'interno della stessa sede è preferibile l'utilizzo delle unità di rete piuttosto che allegare il documento ad un messaggio di posta elettronica;
- sono da evitare altri modi di comunicazione quali ad esempio sistemi di messaging (chat-forum...);
- in caso di ricezione accidentale di messaggi di valenza ufficiale sulle caselle assegnate, gli assegnatari dovranno inoltrarli tempestivamente al destinatario;
- è obbligatorio controllare i file attachment di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti web o Ftp non conosciuti);

Nell'ipotesi in cui la mail debba essere utilizzata per la trasmissione di dati particolari (ex dati sensibili), si raccomanda di prestare attenzione a che:

- l'indirizzo del destinatario sia stato correttamente digitato,
- l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile;
- nel corpo del messaggio sia presente un'intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio.

NAVIGAZIONE IN INTERNET

E' assolutamente vietata la navigazione in internet per motivi diversi da quelli strettamente legati all'attività lavorativa svolta. Al fine di evitare questa situazione, Il CPT della Provincia di Salerno può prevedere l'adozione di uno specifico sistema di blocco o filtro automatico che prevengano determinate operazioni quali l'upload o l'accesso a specifici siti inseriti in una black list.

A titolo esemplificativo, l'utente non potrà utilizzare internet per:

- effettuare qualsiasi genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dal CPT della Provincia di Salerno (Responsabile Interno o Amministratore di Sistema) e con il rispetto delle normali procedure per gli acquisti;
- ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
- partecipare a forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di

bacheche elettroniche e la registrazione in guest books anche utilizzando pseudonimi (o nicknames)
- accesso a caselle web mail di posta elettronica senza specifica autorizzazione

GESTIONE DEI SUPPORTI ROMOVIBILI

I supporti rimovibili, come ad esempio, penne USB o CD riscrivibili, quando contengono dati personali devono essere custoditi in luogo protetto e non accessibile (cassaforte, armadio chiuso a chiave, etc.). Quando non sono più utilizzati devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri Incaricati non autorizzati al trattamento degli stessi dati, soltanto dopo essere stati formattati. Il trasferimento di file contenenti dati personali, dati particolari (ex dati sensibili) e giudiziari su supporti rimovibili, è da eseguire unicamente in via transitoria, ponendo la massima attenzione alla destinazione di trasferimento e cancellando i file appena possibile.