FALEA Edilcassa

Arezzo

MANUALE PRIVACY PER GLI ENTI BILATERLI DELL'EDILIZIA

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

INDICE

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 enti bilaterali del settore edile (Casse Edili/Edilcasse, Scuole Edili/Cpt), da ora in avanti denominati brevemente Ente/Enti.

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 IN MATERIA DI PRIVACY

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

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:

- 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. TRATTAMENTO DEI DATI DEGLI ENTI

3.1 Elenco dei Trattamenti di Dati Personali

L'ambito di applicazione del presente documento riguarda i trattamenti dei dati personali effettuati dagli Enti bilaterali.
L'Ente esegue i trattamenti sia tramite strumenti elettronici, attraverso il proprio sistema informativo, sia attraverso strumenti tradizionali, tramite i propri archivi cartacei.
Tra i trattamenti di dati compiuti dagli Enti, ve ne sono alcuni che riguardano quei dati definiti dal Regolamento come particolari (ex "*sensibili*"). Basti pensare ai dati relativi alla salute e a quelli relativi alle iscrizioni sindacali.
Non è possibile, inoltre, escludere a priori il trattamento di dati "*giudiziari*" nel corso dell'attività di recupero crediti degli Enti.
Presso l'Ente è stato effettuato un censimento degli archivi presso i quali sono registrati dati personali.

3.2 Natura dei dati trattati dall'Ente

L'Ente può trattare sia i dati personali dei propri dipendenti, che quelli degli operai iscritti e dei loro familiari, oltre agli altri (dati di terzi collaboratori, fornitori etc.).

I dati trattati possono essere sia i dati anagrafici/identificativi che i dati particolari.

Le tipologie di dati trattati saranno esemplificate nell'apposito registro dell'attività, unitamente alle finalità e a tutte le altre informazioni richieste dal Regolamento.

3.3 Designazione degli incaricati

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

3.4 Attività degli incaricati

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).

Gli incaricati non sono, in nessun caso, tenuti a comunicare informazioni, circa i lavoratori e le imprese, richieste telefonicamente.

3.5 Procedure operative

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 nell'Ente.

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 associazioni sindacali* 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.

4. ISTRUZIONI PER I TRATTAMENTI SVOLTI CON STRUMENTI ELETTRONICI O COMUNQUE AUTOMATIZZATI

4.1 Istruzione per i trattamenti svolti

La presente sezione di Documento Unico Privacy comprende le istruzioni operative generali relative a:

a) parola chiave per l'accesso ai dati
b) autonoma sostituzione della parola chiave per l'accesso ai dati
c) antivirus e protezione da programmi pericolosi
d) riutilizzo controllato dei supporti
e) autorizzazioni all'ingresso nei locali
f) controllo accesso ai locali
g) trattamenti per fini esclusivamente personali
h) ripristino dati

a) parola chiave per l'accesso ai dati

Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave conosciuta solamente dal medesimo. Il codice per l'identificazione non può essere assegnato ad altri incaricati, neppure in tempi diversi.

La password (o parola chiave):

- non deve essere divulgata e deve essere custodita con la massima diligenza;
- deve essere modificata dall'assegnatario al primo utilizzo e, successivamente, almeno ogni tre/sei mesi.
- deve essere composta da almeno otto caratteri (qualora il sistema lo consenta) e non deve contenere riferimenti agevolmente riconducibili all'incaricato come ad esempio il nome o la data di nascita o loro parti;
- dopo ogni modifica, le nuove credenziali devono essere consegnate in busta chiusa

(recante il nome dell'incaricato al trattamento) firmata agli incaricati della custodia per i casi di emergenza più avanti descritti.

Il nome utente viene generato e comunicato all'inizio della presa di servizio.
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.

Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

Qualora sul disco rigido del PC utilizzato in modalità stand alone siano registrati archivi di dati personali è resa obbligatoria la parola chiave all'accensione del PC.

E' obbligo, per evitare che dati personali possano essere letti da persone non autorizzate, utilizzare la modalità, qualora possibile, dello screen saver con password o disconnettere il pc dalla rete locale (in modo che per utilizzarlo sia necessario inserire la password) quando non è utilizzato (ad es. pausa pranzo).

Gli strumenti devono essere spenti ogni sera prima di lasciare gli uffici (salvo diverse disposizioni o in caso di particolare necessità) presidiando fino al corretto completamento dello spegnimento del sistema.

Nella pausa del pranzo ogni incaricato deve eseguire le seguenti operazioni:

- salvataggio e la chiusura di tutti i file ed applicazioni aperte per non ostacolare eventuali attività di amministrazione;

- blocco dello schermo con la combinazione di tasti "CTRL-ALT- Canc" per evitare di lasciare incustodito l'accesso allo strumento

L'operatore che dovrà effettuare la stampa dei dati è tenuto a ritirarla immediatamente dai vassoi delle stampanti comuni per evitare accessi da parte di persone non autorizzate;

E' fatto assoluto divieto di consentire, a terzi (es. stretti collaboratori) l'accesso ad archivi mediante l'utilizzo della propria parola chiave.

In caso di necessità improrogabile di connessione al sistema informativo attraverso le credenziali di uno specifico incaricato ed in concomitanza all'irreperibilità di quest'ultimo, viene adottata la seguente procedura:

- il custode delle credenziali apre la busta sigillata in suo possesso ed utilizza le credenziali della persona irreperibile;

- al rientro della suddetta persona, si provvederà ad avvisarlo dell'avvenuto intervento e si realizzerà una nuova busta con una diversa password da consegnare al custode delle credenziali.

b) autonoma sostituzione della parola chiave per l'accesso ai dati

La parola chiave è autodeterminata dai singoli soggetti. L'autodeterminazione avviene in seguito alla sostituzione di quella precedentemente assegnata dall' Ente e, successivamente, modificata almeno ogni sei mesi. In caso di trattamento di dati particolari (ex sensibili) la parola chiave è modificata almeno ogni tre mesi.

La parola chiave, in ogni caso, non potrà essere comunicata ad altri soggetti per nessun motivo e non potrà essere trascritta o annotata in maniera evidente o visibile da altri. Nella generazione della parola chiave si dovranno adottare criteri di massima prudenza ad evitare che la stessa possa essere individuata per limitati tentativi. AI riguardo sarà opportuno evitare di comporre la parola chiave con nomi di persona, animali o cose; potrà contenere, casualmente, lettere - meglio se maiuscole e minuscole - e numeri, utilizzando una combinazione minima di otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito. Nel caso di utilizzo di più password queste dovranno essere diverse tra di loro.

c) antivirus e protezione da programmi pericolosi

Tutti i PC dell'Ente connessi in rete devono essere dotati di un programma atto alla rilevazione di virus informatici. Il programma antivirus è installato in modalità residente in memoria, risulta perciò sempre attivo ed aggiornato con la dovuta periodicità (almeno semestrale).
L'amministratore del sistema provvede agli aggiornamenti periodici, alla verifica frequente dell'efficacia del prodotto di prevenzione ed alla impostazione delle opzioni di controllo previste dal programma antivirus. Le opzioni stabilite dall'Ente non possono essere modificate.

Devono essere aggiornati periodicamente, con cadenza almeno annuale, i programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggere difetti. In caso di trattamento di dati particolari (ex sensibili) l'aggiornamento è almeno semestrale.

Si ricorda, con l'occasione, che:

- è fatto divieto assoluto di installare arbitrariamente programmi software non rilasciati ufficialmente dall'Ente; è fatto altresì divieto di importare programmi dalla rete internet se non per uso professionale e strettamente attinente alle funzioni svolte; non sono consentiti l'apertura e l'esecuzione di file in "attachment" alle e-mail ricevute da mittenti sconosciuti;

- è vietato l'accesso a siti internet se non, esclusivamente, per consultazioni di natura professionale; di conseguenza le richieste di connessione potranno riguardare unicamente indirizzi di contenuto adeguato.

- la casella di posta elettronica è messa a disposizione dall'Ente per usi prevalentemente professionali. L'invio di e-mail generalizzato a gruppi (interni o esterni all'Ente) di

soggetti è consentito solo al personale autorizzato da specifiche disposizioni interne.

e) Riutilizzo controllato dei supporti

Gli incaricati debbono custodire e controllare i supporti magnetici o cartacei (es. elenchi, registri, tabulati, fascicoli, ecc. ecc.) sui quali sono registrati i dati particolari in maniera che soggetti non autorizzati non possano venire a conoscenza, nemmeno occasionalmente o accidentalmente, del contenuto di tali supporti. Al termine di ogni lavorazione i supporti in argomento dovranno essere custoditi in appositi contenitori e riposti in armadi o cassetti muniti di serratura e chiusi a chiave.

L'uso e la custodia delle chiavi sono disciplinati dai regolamenti interni delle singole aree di lavoro o secondo le procedure indicate dal Responsabile (ove previsto). I duplicati delle chiavi (se esistono) devono essere custoditi dal Responsabile. E' data facoltà ai soggetti preposti alla custodia di nominare, in presenza di particolari necessità operative e previo benestare del Responsabile del trattamento dei dati personali (ove previsto), un sostituto che sarà considerato temporaneamente preposto alla custodia delle parole chiave. Le chiavi dovranno essere conservate in un armadio, o cassettiera, chiuso a chiave.

I supporti in argomento non dovranno essere utilizzati da altri soggetti che non possiedono l'incarico scritto di poterli trattare. In caso di cattivo funzionamento del supporto che ne determini l'impossibilità della lettura dei dati registrati, i supporti dovranno essere distrutti ovvero smaltiti.

f) Autorizzazione all'ingresso nei locali

L'ingresso nei locali dell' Ente è riservato ai dipendenti e alle persone espressamente autorizzate.

g) Trattamento di dati particolari (ex dati sensibili) per fini esclusivamente personali

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

h) Ripristino dati

Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

i) Uso della Posta Elettronica

L'utilizzo della posta elettronica interna contribuisce fortemente a rendere la comunicazione tempestiva, efficace ed economica. 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;

- per la trasmissione di files 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...)

Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. Pertanto:

- è fatto divieto 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.

- in caso di ricezione accidentale di messaggi di valenza ufficiale sulle caselle assegnate, gli assegnatari dovranno inoltrarli tempestivamente al destinatario.

Relativamente alla navigazione Internet è tassativamente proibito **:**

- scaricare software, anche gratuito, se non per esigenze strettamente professionali, fatti salvi i casi di esplicita autorizzazione dei responsabili del sistema informativo;

- effettuare qualsiasi genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla Direzione 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);

5. ISTRUZIONI PER I TRATTAMENTI SVOLTI CON STRUMENTI DIVERSI DA QUELLI ELETTRONICI O COMUNQUE AUTOMATIZZATI

5.1 Istruzione per i trattamenti svolti

La presente sezione di Documento Unico Privacy comprende le istruzioni operative generali relative a:

a) accesso dati
b) conservazione in archivi ad accesso selezionato
c) custodia atti e documenti

d) restituzione atti e documenti al termine delle operazioni
e) conservazione in contenitori muniti di serratura
f) accesso controllato agli archivi
g) custodia e conservazione delle riproduzioni
h) macero e/o distruzione di supporti cartacei contenenti dati personali

a) Accesso ai soli dati necessari

Durante lo svolgimento di trattamenti di dati personali di qualunque natura (particolari e non particolari), registrati su carta o altri supporti, i singoli incaricati delle diverse operazioni di trattamento devono operare solo su quei dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti previsti per le specifiche attività attribuite alla funzione ricoperta.

b) Conservazione in archivi ad accesso selezionato

L'accesso agli archivi contenenti atti e i documenti di dati personali di qualunque natura (particolari e non) è riservato alle sole persone incaricate ed autorizzate a potervi accedere.

c) Custodia atti e documenti

Gli atti e i documenti contenenti dati personali di qualunque natura (particolari e non), devono essere trattati con diligenza, custoditi e conservati in maniera che le persone non incaricate non possano venirne a conoscenza.

Gli incaricati abilitati al trattamento di dati provenienti (o direttamente tratti) da archivi ad accesso selezionato, devono conservare e custodire i dati trattati con diligenza e riservatezza evitando che vengano volontariamente o involontariamente conosciuti da soggetti privi della stessa qualificazione di incaricato.

d) Restituzione atti e documenti al termine delle operazioni

Gli atti e i documenti devono essere trattenuti solo per il periodo strettamente necessario allo svolgimento delle operazioni inerenti i propri compiti e al termine di dette operazioni devono essere restituiti o riposti nell'archivio dal quale erano stati prelevati (o presso il quale devono essere custoditi). Nel Registro dei dati dovrà essere indicata per ogni trattamento il termine di conservazione relativo ai dati.

e) Conservazione in contenitori muniti di serratura

Nel caso vengano svolte operazioni di trattamento di dati particolari (ex sensibili), gli incaricati del trattamento cui sono affidati atti e documenti, oltre a rispettare le norme generali previste per la custodia, dovranno conservare tali atti e documenti, fino alla restituzione, in contenitori (armadi e/o cassetti), muniti di serratura e chiusi. L'accesso ai contenitori è riservato solo alle persone autorizzate a svolgere le stesse operazioni di trattamento. La gestione delle chiavi avviene secondo i regolamenti delle aree e funzioni specifiche.

f) Accesso controllato agli archivi

L'accesso agli archivi contenti atti e documenti di dati particolari (ex sensibili) viene controllato dal personale incaricato appartenente alla funzione di competenza.

g) Custodia e conservazione delle riproduzioni (fotocopie, tabulati, ecc.)

I supporti non informatici contenenti la riproduzione di informazioni relative al trattamento di dati personali particolari (ex sensibili) devono essere custoditi con le stesse modalità previste, dal presente Documento Unico Privacy, per i trattamenti degli atti e i documenti originali.

h) Macero e/o distruzione di supporti cartacei contenenti dati personali

Gli incaricati del trattamento hanno il compito di curare che l'inoltro al macero di supporti cartacei contenenti dati personali (es. tabulati contenenti: dati anagrafici) sia preceduto da idonei interventi ed accorgimenti atti ad evitare che altri soggetti vengano a conoscenza, anche accidentalmente, dei dati riportati sui supporti.

6. TIPOLOGIA DEI DATI E FINALITA' DEL TRATTAMENTO DEI LAVORATORI ISCRITTI ALLE CASSE EDILI/EDILCASSE (REPLICABILE PER GLI ALTRI ENTI)

6.1 Natura dei dati trattati dalla Cassa Edile/Edilcassa

La Cassa Edile può trattare sia i dati personali dei propri dipendenti, che quelli degli operai iscritti e dei loro familiari, oltre agli altri (dati di terzi collaboratori, dei fornitori etc.).

La Cassa Edile/Edilcassa tratta sia dati anagrafici/identificativi che dati particolari, quali ad esempio i dati relativi alla salute dei lavoratori e alle iscrizioni al sindacato.

6.2 Modalità di Trattamento dei dati relativi ai lavoratori iscritti

I dati dei lavoratori iscritti alla Cassa Edile sono trattati sia su supporti cartacei, sia su supporti elettronici.

(*Indicare dove vengono trattati gli archivi automatizzati. Es. server, rete locale,….).*

6.2 Fonte di Raccolta Dati dei lavoratori iscritti alla Cassa Edile

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 l'interessato tramite i moduli d'iscrizione, denunce mensili, dichiarazioni, domande per prestazioni assistenziali extracontrattuali e deleghe sindacali;

La tipologia dei dati personali richiesti, o acquisiti, sia all'atto dell'iscrizione alla Cassa Edile/Edilcassa, sia in una fase successiva, è la seguente:

- dati anagrafici: nominativo, indirizzo ed altri elementi di identificazione personale, dati bancari e postali, e-mail , cellulare, social
- dati familiari: i dati relativi alla 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.

Il trattamento dei dati ha come finalità quella di accertare l'adempimento agli obblighi contrattuali e di legge da parte delle imprese iscritte alla Cassa Edile/Edilcassa e di consentire l'esercizio dell'attività della Cassa stessa.

Tra gli obblighi contrattuali e di legge maggiormente significativi rileviamo:

- la corresponsione del trattamento economico spettante agli operai per le ferie e per la gratifica natalizia;
- la corresponsione agli operai (tramite l'impresa) di un'integrazione al trattamento economico nei casi di malattia ed infortunio sul lavoro;
- la riscossione delle quote e dei contributi sindacali;
- la corresponsione agli operai dell'anzianità professionale edile;
- la corresponsione agli operai delle altre prestazioni previdenziali ed assistenziali previste dal Documento Unico Privacy della Cassa Edile/Edilcassa;
- la riscossione dei contributi per la previdenza complementare;
- l'attuazione dei contratti ed accordi collettivi di riferimento

6.3 Istruzione sul trattamento dei dati particolari

Per tutti i trattamenti che hanno ad oggetto l'adesione ad un sindacato del lavoratore iscritto alla Cassa Edile/Edilcassa, è fatto divieto agli incaricati e/o ai responsabili del trattamento coinvolti, in caso di richiesta da parte del sindacato, di fornire liste o nominativi dei lavoratori iscritti alla Cassa aderenti ad un sindacato diverso da quello di appartenenza del lavoratore.

E' altresì contrario alle disposizioni di legge e al contenuto del presente documento, fornire notizie in merito ai lavoratori non aderenti ad alcun sindacato.

6.4 Comunicazione e divulgazione dei dati a Enti Paritetici di settore e Organizzazioni Datoriali e Sindacali

Ai fini della comunicazione e/o divulgazione dei dati agli Enti Paritetici e alle Organizzazioni Datoriali e Sindacali, sia in forma cartacea che informatica, i destinatari devono essere nominati "Responsabili esterni" del trattamento dei dati.

Tale comunicazione e/o divulgazione deve avvenire dietro richiesta preventiva del

destinatario e previa sottoscrizione di una apposita clausola contrattuale (anche atto di nomina Responsabile esterno quando non contrattualizzato) circa le modalità di trattamento dei dati.

E' consentita la comunicazione e/o diffusione di dati anonimi e aggregati per fini statistici.

6.5 Destinatari della Comunicazione dei dati

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

- alle Pubbliche Amministrazioni che richiedano informazioni alla Cassa Edile in ottemperanza ad obblighi di legge
- agli Enti di previdenza come INPS, Inail e Fondi previdenza complementare
- agli Istituti bancari e finanziari che intrattengono rapporti con la Cassa Edile
- alle Società di servizio per la realizzazione delle finalità della Cassa Edile
- alle altre Casse Edili e loro organismi di coordinamento
- agli altri Enti paritetici di categoria
- alle Associazioni imprenditoriali e sindacali
- alla Società di revisione contabile
- ai Legali e altri consulenti esterni della Cassa Edile/Edilcassa
- ai componenti del Comitato di gestione e del Collegio sindacale
- alle Società assicurative.

Si rinvia al *Registro del Trattamento* dei dati personali per l'individuazione dei nominativi dei terzi destinatari della comunicazione dei dati trattati dalla Cassa.

6.6 Protezione delle Aree e dei Locali

L'obiettivo è la definizione di misure di sicurezza per la predisposizione e il mantenimento di un ambiente di lavoro protetto. Vengono individuate le seguenti modalità:

Il Titolare del Trattamento e il Responsabile del Trattamento mettono in atto misure tecniche e organizzative tese a:

- classificare delle aree funzionali protette da "codici di identificazione" per l'accesso e password ovvero di creare adeguate procedure di accesso controllato ai dati;
- predisporre, e conservare in luogo chiuso e protetto, per ogni incaricato al trattamento una busta nella quale vengono riportati il codice di identificazione e la password;
- revocare tutte le password non utilizzate per un periodo superiore a sei mesi o comunque a soggetti non più autorizzati ad accedere ai dati;
- collocare l'hardware in locali non accessibili al pubblico e a persone non autorizzate;
- impedire l'intrusione nei locali che gli sono stati affidati in custodia da parte di persone non autorizzate;
- impedire il danneggiamento, la manomissione, la sottrazione, la distruzione o la copia di dati nei locali che gli sono stati affidati in custodia da parte di persone non autorizzate;
- conservare i documenti contenenti i dati in contenitori muniti di serratura;

- identificare e registrare i soggetti ammessi dopo l'orario di chiusura degli uffici stessi (es. impresa di pulizie);
- porre in essere dispositivi anti incendio e dispositivi anti intrusione.

6.7 Integrità dei Dati

Le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile hanno accesso ai soli dati personali la cui conoscenza è strettamente necessaria per adempiere ai compiti loro assegnati e si attengono ad una serie di istruzioni.

7. MODALITA' DI ACCESSO AI DATI

Gli accessi agli oggetti del sistema informativo avvengono esclusivamente secondo modalità prestabilite.

Gli incaricati del trattamento dei dati ricevono le abilitazioni in modo da poter accedere ai soli dati necessari per l'espletamento delle mansioni assegnate. Si collegano al sistema attraverso un codice identificativo personale ed una parola chiave.

Il codice è composto ***(indicare la composizione del codice identificativo utente)***. Lo stesso codice non può essere assegnato a persone diverse.

I codici identificativi personali sono assegnati e gestiti in modo da prevedere la disattivazione in caso di perdita della qualità che consente l'accesso all'elaboratore, o di mancato utilizzo dei medesimi per un periodo superiore a 6 mesi.

La parola chiave è strettamente personale e non viene comunicata a estranei.

La lunghezza della parola chiave è quella massima consentita dal sistema, pari a ***(indicare il numero di caratteri, ferma restando la lunghezza minima di otto caratteri alfanumerici).***.

Le password vengono modificate ogni sei mesi ad eccezione di quelle utilizzate dagli incaricati al trattamento dei dati particolari (ex sensibili) che prevedono una modifica trimestrale.

8. Criteri e modalità di ripristino della disponibilità dei dati

Il piano di continuità operativa rappresenta l'aspetto della sicurezza principalmente orientata a garantire la continuità e la disponibilità dei sistemi informativi automatizzati rispetto a danneggiamenti causati da eventi accidentali, sabotaggi e disastri naturali.

Come già sopra evidenziato esiste una procedura di salvataggio degli archivi.

(Indicare la periodicità dei salvataggi, il tipo di salvataggio, i supporti utilizzati, il numero di copie e ubicazione delle stesse, la struttura operativa o persona incaricata del salvataggio)

Vengono poste in essere procedure idonee a garantire l'organizzazione e la custodia della documentazione cartacea gestita dall'Ente in archivi ad accesso autorizzato e sotto il diretto controllo del Responsabile del trattamento.

(Indicare l'eventuale presenza di dispositivi di continuità elettrica con tempi di funzionamento garantiti).

9. MISURE DI SICUREZZA

Di seguito sono elencate alcune notazioni riguardo l'adozione delle misure tecniche e organizzative di sicurezza così come previste nel Regolamento UE 2016/679.

9.1 Misure per trattamenti informatici

- Tutti gli incaricati sono dotati di credenziali di autenticazione (codice identificativo personale e parola chiave). Il trattamento dei dati personali richiede il superamento di una o più procedure di autenticazione, per l'accesso alla rete e/o all'applicazione.

- L'Amministratore di sistema e/o il Responsabile del Trattamento dell'Ente provvede ad operazioni periodiche di pulizia degli account per disattivare credenziali inutilizzate, o riferite ad incaricati che hanno perso le qualità per accedere ai dati personali.

- In caso di necessità improrogabile il custode delle credenziali, che svolge anche la mansione di amministratore di sistema, sostituisce la parola chiave dell'incaricato con una nuova senza bisogno di conoscere la vecchia. Questo garantisce l'impossibilità per lo stesso di collegarsi ai sistemi usando l'identità dell'incaricato senza compiere azioni che non risultino evidenti all'incaricato stesso. Infatti, al suo rientro in azienda l'incaricato non riuscirà a connettersi con la sua vecchia parola chiave, risultando quindi automaticamente avvisato dell'avvenuto intervento, che in ogni caso si provvederà a comunicare. Questo metodo garantisce inoltre la relativa segretezza della password.

In caso di assenza dell'operatore le sessioni di trattamento vengono preventivamente chiuse dall'operatore stesso.

- Su tutti i personal computer sono installati software "Internet security" che si aggiornano ***giornalmente.***

- L'evoluzione dei sistemi operativi delle workstation e dei client viene monitorata regolarmente. Gli aggiornamenti tramite patch software sono effettuati ***mensilmente.***

- L'Ente tratta i dati relativi allo stato di salute dei lavoratori e dei dipendenti custodendoli in appositi archivi protetti, controllando che ad essi non accedano persone prive di autorizzazione.

9.2 Misure per trattamenti cartacei

- L'ingresso nei locali dell'Ente non aperti al pubblico è riservato ai dipendenti e alle persone espressamente autorizzate.

- Nei locali in cui vengono svolti trattamenti di dati particolari possono accedere solo gli incaricati espressamente autorizzati; è consentito l'accesso ad altre persone solo in presenza degli incaricati o del Responsabile del trattamento interno (ove esistente) dell'Ente.

- L'accesso alle stanze archivio è consentito alle sole persone incaricate ed autorizzate a potervi accedere e viene controllato dal Responsabile del trattamento interno (ove esistente).

- Gli incaricati del trattamento di dati personali, oltre a rispettare le norme generali previste per la custodia (diligenza), sono tenuti a conservare atti o documenti in contenitori (armadi e/o cassetti) muniti di serratura e chiusi; l'accesso a tali contenitori è consentito solo alle persone autorizzate a svolgere le operazioni di trattamento.

10. MISURE DI SICUREZZA IN CASO DI TRATTAMENTO DI DATI PERSONALI AFFIDATI A TERZI

10.1 Responsabile esterno del trattamento

Qualora il trattamento dei dati debba essere effettuato 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 del 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. Le clausole contrattuali stipulate con i Responsabili esterni contengono un protocollo per l'effettuazione delle suddette verifiche.

(nel Registro dell'attività dei trattamenti saranno indicati: l'attività esternalizzata, i dati interessati, il nominativo del soggetto esterno; gli impegni assunti dal soggetto stesso per garantire un adeguato trattamento dei dati).

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.

11. MISURE DI SICUREZZA TECNICHE: MISURE INFORMATICHE, CARTACEE E LOGISTICHE E SISTEMI DI VIDEOSORVEGLIANZA

In generale, un sistema informativo si definisce sicuro quando soddisfa i seguenti requisiti:

- **Disponibilità**: l'informazione ed i servizi che eroga devono essere disponibili per gli utenti coerentemente con i livelli di servizio;
- **Integrità**: l'informazione ed i servizi erogati possono essere creati, modificati, o cancellati solo dalle persone incaricate a svolgere tale operazione;
- **Confidenzialità o Riservatezza**: l'informazione può essere utilizzata solo dalle persone

incaricate a compiere tale operazione.

- **Custodia e controllo:** i dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non conforme alle finalità della raccolta.

11.1 Verifiche periodiche sulle misure di sicurezza informatiche, cartacee e logistiche

Qui di seguito sono elencate le principali verifiche circa l'applicazione delle misure di sicurezza informatiche, cartacee e logistiche:

Misure da verificare	**Descrizione Misura**	**Termine o periodicità**
Parola chiave	Per il trattamento di dati personali deve essere modificata ogni sei mesi	6 mesi
Parola chiave	Per il trattamento di dati particolari (ex sensibili) e giudiziari deve essere modificata ogni tre mesi	3 mesi
Codice per l'identificazione	Una volta assegnato, non può essere assegnato ad altri incaricati	sempre
Credenziali di autenticazione	Disattivazione in caso di mancato utilizzo per un periodo superiore ai 6 mesi	6 mesi
Credenziali di autenticazione	Disattivazione in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali	sempre
Profili di autorizzazione	Possono essere individuati per singolo incaricato o per classi omogenee di incaricati	sempre
Profili di autorizzazione	Verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione	1 anno
Lista degli incaricati autorizzati	Può essere redatta anche per classi omogenee di incarico	1 anno
Antivirus	Efficacia ed aggiornamento sono verificati con cadenza almeno semestrale	6 mesi
Patch o programmi update	Programmi per elaboratore volti a correggere difetti e prevenire la vulnerabilità degli strumenti elettronici	1 anno
Patch o programmi update	Programmi per elaboratore volti a correggere difetti e prevenire la vulnerabilità degli strumenti	6 mesi

	elettronici (dati particolari - ex sensibili e giudiziari)	
Backup	Salvataggio dei dati con frequenza settimanale	7 giorni

Formazione incaricati	Ingresso, cambiamento mansioni, nuovi strumenti	sempre
Sistemi anti intrusione	Protezione contro l'accesso abusivo nel caso di trattamento di dati particolari	sempre
Supporti rimovibili	Istruzioni per custodia e uso (dati particolari)	sempre
Supporti rimovibili	Istruzioni in caso di non uso (dati particolari)	sempre
Ripristino accesso dati	Ripristino accesso dati in caso di danneggiamento degli stessi o degli strumenti elettronici (dati particolari e giudiziari)	massimo 7 giorni

11.2 Descrizione del sistema informatico

L'Ente dispone della seguente architettura hardware:

(indicare la descrizione del sistema informativo esistente: tipo macchine dove risiedono i dati principali, numero personal computer e terminali, numero stampanti, dislocazione fisica delle macchine, esistenza di password, accesso a posta elettronica, esistenza di antivirus, dislocazione dei dati trattati, modalità dei salvataggi)

(tipologia della rete: specificare se di tipo bus, stellare o altro)

(tipo di connessione ad Internet: specificare se connessione ADSL, ISDN, altro, tramite modem o router)

INVENTARIO HARDWARE (a titolo esemplificativo)	
(indicare quantità di) Personal Computer con sistema - operativo Windows 10 n. 4 personal computer n. 1 portatile	Scopi di Videoscrittura, Scopi di amministrazione e Segreteria, e-mail

Num. x monitor 1	Monitor
Num. x telefoni 6	Telefoni
Num. x Firewall	Protezione da attacchi esterni
Num. x Router 1	Collegamento Internet
Num. x Stampanti	Periferiche uscite stampati
Num. x Server – San 3	VmWare - nodi ESXi - storage esterno SAN HyperV - nodi Microdoft Windows Server - SAS – SAN
Num. x NAS	Salvataggio dati
Num. x Access Point	Access WiFi
Num. x switch	Collegamento postazioni di lavoro e server
Num. x centralini telefonici	Centralini telefonici

INVENTARIO SOFTWARE	
Gestione Contabilità	Indicare software (Data Proget Srl) Indicare software (Data Proget Srl)
Gestione Anagrafiche	Indicare software (Data Proget Srl) Indicare software (Data ProgetSrl)
E-Banking	Indicare software UBI Banca Poste Italiane
Comunicazioni consulente Buste Paga	Indicare software CNA Arezzo

11.3 Rete Locale - Descrizione generale delle caratteristiche del sistema informativo aziendale

N.B. LA SEGUENTE DESCRIZIONE HA SOLO SCOPO ESEMPLIFICATIVO

I dispositivi informatici utilizzati per il trattamento dei dati dell'Ente in qualità di titolare del trattamento sono connessi tra loro attraverso una rete locale Ethernet su protocollo TCP/IP,

dislocata nelle seguenti sedi operative:

1. Arezzo: sede principale, che ospita uffici amministrativi:

Presso tale sede sono presenti anche le seguenti connessioni wi-fi:
- Tramite router TIM
- Uffici: consente l'accesso attraverso credenziali di tipo WPA2, gestite dall'Amministratore di Sistema che le configura solo previa identificazione dell'interessato
- Ospiti: segregata da specifica VLAN, accessibile da tutti gli ospiti previa configurazione, permette l'esclusiva connettività verso l'esterno di alcune porte del firewall

Inoltre è possibile accedere all'infrastruttura aziendale attraverso VPN assegnate a dipendenti e fornitori autorizzati (DATA PROGET), di cui è mantenuto l'elenco aggiornato a cura di Rossi Remo

Tale rete è amministrata da una serie di computer Server (sistemi fisici) che si occupano di fornire i servizi di rete necessari ai clienti.

I server sono dislocati presso la Sede, debitamente attrezzati con dispositivi UPS e impianto di condizionamento:

- Gestionale: riservato ai server gestionali (tre) è realizzato con tecnologia IBM AS 400

L'accesso ai CED è riservato al solo personale autorizzato con apposita chiave.
La configurazione standard dei client prevede le seguenti configurazioni:

- I programmi gestionali sono accessibili tramite accesso nominale protetto
- è installato software antivirus mantenuto costantemente aggiornato attraverso una procedura automatizzata
- i dati contenuti dai server sono giornalmente salvati attraverso dispositivi rimovibili conservati in armadietto ignifugo e talvolta portati precauzionalmente all'esterno

Le tipologie dei client sono le seguenti:
- uffici: il client è assegnato univocamente all'incaricato, dotato di credenziali di accesso univoche.

11.6 Schedari e supporti cartacei

Nella sede di Arezzo tutta la documentazione cartacea viene raccolta in schedari, i quali vengono custoditi i armadi dotati di chiavi.

11.7 Misure logistiche

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 di continuità di alimentazione

Dispositivo	Si	No	% di locali
Sistema UPS	X		15
Inverter per stabilizzazione		X	100
Gruppo elettrogeno		X	100

Presenza di dispositivi infrastrutturali

Dispositivo	Si	No	% di locali
Armadi ignifughi e stagni	X		15
Quadro elettrico chiuso a chiave	X		
Armadio per i dispositivi di fonia e dati chiuso a chiave		X	
Estintori	X		20

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	100

12. VALUTAZIONE DEL RISCHIO

Valutazione rischio per ogni area (minimo, medio, massimo in questa fase: necessaria valutazione insieme a funzione IT e a seguito dell'inventario hardware/software).

Ai sensi dell'Articolo 32 del Regolamento (UE) 2016/679, relativo alla sicurezza del trattamento dei dati, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.
Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

L'Ente ha effettuato in tal senso la seguente analisi dei rischi inerenti al trattamento dei dati personali.

In conformità allo standard sono stati considerati i rischi che possono agire distintamente sulle proprietà di Confidenzialità, Disponibilità e Integrità che devono essere possedute dell'informazione.

I rischi ricorrenti connessi al trattamento dei dati per gli Enti sono i seguenti:

- Distruzione e perdita dei dati, dovuti a furto di strumenti o credenziali di autorizzazione, guasti, sabotaggi, inaffidabilità dei supporti fisici, deterioramento nel tempo, eventi naturali quali allagamenti e incendi.

- Accesso non autorizzato: rischio che persone non incaricate abbiano accesso agli archivi automatizzati e/o cartacei contenenti dati personali.

- Trattamento non consentito o non conforme alle finalità: errori involontari, codici "maliziosi", attacchi mirati a rendere indisponibile un servizio, modifiche deliberate o accidentali.

(Indicare per ciascun rischio la contromisura adottata/da adottare in relazione alla gravità stimata)
In particolare:

TRATTAMENTO	RISCHI SPECIFICI INERENTI I DATI (Da scegliere tra uno o più dei seguenti esempi)	MISURE DI SICUREZZA E TIPO DI PROCESSO A CUI I DATI SONO SOTTOPOSTI	VALUTAZIONE DEL RISCHIO
Trattamenti per finalità di gestione del personale dell'Ente	Perdita Distruzione Divulgazione non autorizzata Utilizzo improprio Rischio specifico: divulgazione dati aziendali in grado di rivelare inadempienze	Documento Unico Privacy (Richiamando tra i seguenti ESEMPI): - Accessi riservati al solo personale autorizzato - Protezione archivi informatici tramite parole d'accesso fornite dal gruppo direzione e poi oggetto di autenticazione. - Esistono due regolamenti informatici (Internet e posta + Utilizzo VPN) - Protezione fisica dei documenti inseriti in archivi cartacei in gestione all'Uff. Amministrativo (Paola Troiani) - Installazione di un software antivirus e previsione di backup sui server. - Procedura di back up dei dati periodici - Inventario hardware e software - Aggiornamento annuale dei software e hadware	All'esito della analisi informatica Minimo/medio/ massimo
Formazione del personale dell'Ente	Perdita Distruzione		

	Divulgazione non autorizzata Utilizzo improprio Rischio specifico: divulgazione dati aziendali in grado di rivelare inadempienze		
Gestione operai iscritti	Perdita Distruzione Divulgazione non autorizzata Utilizzo improprio Rischio specifico: divulgazione dati aziendali in grado di rivelare inadempienze		
Sicurezza (D.Lgs. 81/2008)	Perdita Distruzione Divulgazione non autorizzata Utilizzo improprio Rischio specifico: divulgazione dati aziendali in grado di rivelare inadempienze		
Gestione fornitori	Perdita Distruzione Divulgazione non autorizzata Utilizzo improprio Rischio specifico: divulgazione dati aziendali in grado di rivelare inadempienze		
Adempimenti previsti dalla normativa 231/2001 (solo per gli Enti che hanno adottato il modello)	Perdita Distruzione Divulgazione non autorizzata Utilizzo improprio Rischio specifico: divulgazione dati aziendali in grado di rivelare inadempienze		
Controlli di qualità (SOLO PER CPT)	Perdita Distruzione Divulgazione non autorizzata Utilizzo improprio Rischio specifico: divulgazione dati aziendali in grado di rivelare inadempienze		
Gestione informatica e sicurezza informatica	Perdita Distruzione Divulgazione non autorizzata Utilizzo improprio Rischio specifico:		

	divulgazione dati aziendali in grado di rivelare inadempienze		

13. 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 debba 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. SPECIFICARE LE MODALITA' DI INTERVENTO IT (OPPURE ALMENO RICHIAMARE QUI IL NOME DEL CONSULENTE IT CHE PORRA' IN ESSERE L'INTERVENTO)

Comunicazione all'interessato (N.B. La forma è libera)
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 non è tuttavia richiesta nei seguenti casi:

- La prima ricorre 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).
- La seconda è prevista 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.

- La terza si presenta 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.

LA PARTE CHE SEGUE E' A SOLO SCOPO INFORMATIVO E NON VA RIPORTATA NEL DOCUMENTO UNICO

In sostanza, dunque, è opportuno procedere a un duplice controllo.

Da un lato, occorre verificare che siano state adottate le misure di protezione adeguate, così da poter stabilire se c'è stata violazione dei dati personali e informare, di conseguenza, l'autorità di controllo e gli interessati.

Dall'altro, si deve stabilire se la notifica è stata trasmessa senza ingiustificato ritardo, tenendo conto, in particolare, della natura e della gravità della violazione, nonché delle sue conseguenze ed effetti negativi per l'interessato.