



DOCUMENTO UNICO PRIVACY DELLA CASSA EDILE DELLA PROVINCIA DI NAPOLI

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

INDICE

1.	PREMESSA	3
2.	DEFINIZIONI IN MATERIA DI PRIVACY	4
3.	TRATTAMENTO DEI DATI DEGLI ENTI.....	8
3.1	Elenco dei Trattamenti di Dati Personali	8
3.2	Natura dei dati trattati dall'Ente	8
3.3	Designazione degli incaricati.....	8
3.4	Attività degli incaricati	8
3.5	Procedure operative	9
4.	ISTRUZIONI PER I TRATTAMENTI SVOLTI CON STRUMENTI ELETTRONICI O COMUNQUE AUTOMATIZZATI	9
4.1	Istruzione per i trattamenti svolti	9
5.	ISTRUZIONI PER I TRATTAMENTI SVOLTI CON STRUMENTI DIVERSI DA QUELLI ELETTRONICI O COMUNQUE AUTOMATIZZATI	14
5.1	Istruzione per i trattamenti svolti	14
6.	TIPOLOGIA DEI DATI E FINALITA' DEL TRATTAMENTO	16
6.1	Natura dei dati trattati dalla Cassa Edile	16
6.2	Modalità di Trattamento dei dati relativi ai lavoratori iscritti	16
6.2	Fonte di Raccolta Dati dei lavoratori iscritti alla Cassa Edile	16
6.3	Istruzione sul trattamento dei dati particolari.....	17
6.4	Comunicazione e divulgazione dei dati a Enti Paritetici di settore e Organizzazioni Datoriali e Sindacali	17
6.5	Destinatari della Comunicazione dei dati	17
6.6	Protezione delle Aree e dei Locali.....	18
6.7	Integrità dei Dati	18
7.	MODALITA' DI ACCESSO AI DATI.....	19
8.	CRITERI E MODALITÀ DI RIPRISTINO DELLA DISPONIBILITÀ DEI DATI	19
9.	MISURE DI SICUREZZA IN CASO DI TRATTAMENTO DI DATI PERSONALI AFFIDATI A TERZI	20
9.1	Responsabile esterno del trattamento	20
10.	MISURE DI SICUREZZA TECNICHE: MISURE INFORMATICHE, CARTACEE E LOGISTICHE E SISTEMI DI VIDEOSORVEGLIANZA.....	21
10.1	Requisiti del sistema informativo	21
10.2	Misure di sicurezza generali.....	21
10.3	Misure per trattamenti informatici.....	21
10.4	Misure per trattamenti cartacei	22
10.5	Verifiche periodiche sulle misure di sicurezza informatiche, cartacee e logistiche	22
	Termine o periodicità.....	22
10.6	Descrizione del sistema informatico	24
10.7	Rete Locale - Descrizione generale delle caratteristiche del sistema informativo aziendale	25
10.8	Videosorveglianza: valutazione sulle necessità e finalità del trattamento	27
10.9	Descrizione del sistema di videosorveglianza.....	27
10.10	Schedari e supporti cartacei	29
10.11	Misure logistiche	29
11.	VALUTAZIONE DEL RISCHIO	35
12.	NOTIFICA IN CASO DI DATA BREACH	44



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 e ha ad oggetto il trattamento dei dati svolti dalla Cassa Edile della Provincia di Napoli CASSA EDILE DI NAPOLI Viale della Costituzione, C.D.N. Isola F/3 - 80143 NAPOLI tel.081 734 71 36(PBX) - fax 081 734 71 38.

I dati di contatto del Data Protection Officer sono: avv. Maurizio Cappabianca, mail: dpo@cassaedilenapoli.it; mauriziocappabianca@avvocatinapoli.legalmail.it contatto telefonico +393312145249.

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;
- destinatari 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.



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.

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) così 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 concisa, 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);



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.



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:

-  parola chiave per l'accesso ai dati
-  autonoma sostituzione della parola chiave per l'accesso ai dati
-  antivirus e protezione da programmi pericolosi
-  riutilizzo controllato dei supporti
-  autorizzazioni all'ingresso nei locali
-  controllo accesso ai locali
-  trattamenti per fini esclusivamente personali
-  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. Al 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 cassette 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 benessere 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 cassettera, 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);



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 tratti 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 casseti), 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 contenenti 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.



TIPOLOGIA DEI DATI E FINALITÀ DEL TRATTAMENTO

6.1 Natura dei dati trattati dalla Cassa Edile della Provincia di Napoli

La Cassa Edile può trattare sia i dati personali dei propri dipendenti, degli operai iscritti e dei loro familiari, dei rappresentanti delle imprese, dei committenti persone fisiche ai sensi dell'allegato 17 del D.Lgs 81/08 per l'attività della notifica preliminare, oltre ai dati di terzi collaboratori, fornitori e consulenti.

La Cassa Edile 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

I dati dei lavoratori iscritti alla Cassa Edile sono trattati sia su supporti cartacei, sia su supporti elettronici nelle banche dati individuate al capitolo 10 del presente documento.

6.2 Fonte di Raccolta Dati dei lavoratori iscritti alla Cassa Edile


I dati sono raccolti secondo le seguenti modalità:

- In esecuzione del contratto di lavoro o in adempimento di un obbligo di legge (D.lgs. 81/08) con il dipendente della Cassa;
- In esecuzione dei Contratti Collettivi Nazionali del Lavoro Settore Edilizia (per le prestazioni contrattuali) e in esecuzione del contratto territoriale (per le prestazioni extracontrattuali) per i dati del lavoratore iscritto, mediante comunicazione da soggetti diversi dall'interessato, ovvero mediante comunicazioni inviate dalle imprese;
- In adempimento di un obbligo di legge (allegato 17 del D.Lgs 81/08) nel caso della notifica preliminare avente ad oggetto il dato del committente persona fisica;
- Mediante e in esecuzione di contratto con i fornitori di beni o servizi.

La tipologia dei dati personali richiesti, o acquisiti, sia all'atto dell'iscrizione alla Cassa Edile, 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: stato di salute adesione ad un sindacato.
- ogni altro dato utile o indispensabile per la applicazione della contrattazione collettiva di settore.

Il trattamento dei dati ha le seguenti finalità:

 per i dipendenti della Cassa, la gestione delle attività di protocollo della documentazione, l'amministrazione gestione del personale, il pagamento stipendi/emolumenti, la verifica

congruità pagamento delle note spese, la gestione delle assunzioni/collaborazioni/dimissioni / licenziamenti/ dei trattamenti pensionistici, delle astensioni obbligatorie e/o facoltative /assistenzialistici /fiscali / assicurativi; l'attività di payroll, detrazioni fiscali , trattamenti ex L. 104/1992, esoneri, permessi retribuiti, congedi; la rilevazione e la normalizzazione delle presenze, la gestione di visite mediche periodiche al personale dipendente per idoneità alla mansione, la formazione del personale dipendente e non dipendente e gli adempimenti di cui al DLgs 81/2008, art. 26 inerenti contratti di appalto con clienti, rischi da interferenza e somministrazione lavoro; la gestione autorizzazioni di accesso al sistema informatico e relativa ai profili utente; la gestione delle attività finalizzate ad assicurare l'integrità, la disponibilità e la sicurezza dei dati trattati con mezzi automatizzati;

🔗🕒 per i lavoratori iscritti, la gestione dell'attività di protocollo, la liquidazione degli accantonamenti e la liquidazione dell' A.P.E. (anzianità professionale edile), la gestione di rimborsi malattia/infortunio, la liquidazione prestazioni facoltative, la Assistenza e D.P.I., gestione dei Servizi di previdenza e mutualità, corresponsione contributi extracontrattuali, gestione delle Attività di recupero credito, corresponsione quote e contributi sindacali, gestione del rimborso Fondo Prevedi, attuazione accordi collettivi di riferimento, rilascio della certificazione della regolarità contributiva, emissione del MUT con cadenza mensile, gestione dell'iscrizione ad un Sindacato in seguito a Delega;

🔗🕒 per fornitori e i consulenti, l'inserimento in registri / elenchi di fornitori necessari per la gestione del rapporto con fornitore, la gestione rapporto commerciale con fornitore di prodotti o servizi (invio corrispondenza, stipula contratti), l'utilizzo dati per fatturazione/Rapporti commerciale e in generale, ai fini del corretto adempimento degli obblighi contrattuali.

Tra gli obblighi di legge maggiormente significativi rileviamo:

- l'attuazione dei contratti ed accordi collettivi di riferimento;
- Il D.lgs. 81/08 in materia di salute e sicurezza sul lavoro;
- L'allegato 17 del D.Lgs 81/08 per la notifica preliminare.

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, 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

PER IL LAVORATORE ISCRITTO:

I dati trattati non verranno comunicati a soggetti privi di autorizzazione concessa dal Titolare, fatta salva la comunicazione o diffusione di dati richiesti, in conformità alla legge, da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici per finalità di difesa o di sicurezza dello Stato, di prevenzione, di accertamento o repressione dei reati. I predetti dati sono altresì a disposizione degli Amministratori in carica, limitatamente alla loro funzione di amministratori dell'Ente.

I dati conferiti potranno essere comunicati al fine di consentire l'adempimento degli obblighi contrattuali o di legge, per le finalità sopra elencate, a:

- tutti i soggetti cui la facoltà di accesso a tali dati è riconosciuta in forza di provvedimenti normativi e giudiziali, ad esempio organi di Polizia e Pubblica Amministrazione in genere;
- ai dipendenti e ai collaboratori incaricati e autorizzati, nell'ambito delle relative mansioni, a trattare i dati forniti;
- a tutte quelle persone fisiche e/o giuridiche, pubbliche e/o private, esterne alla Cassa Edile ma alle quali la comunicazione dei Suoi dati risulti necessaria o funzionale alle finalità predette, in particolare:
 - alle Casse di previdenza ed assistenza, come INPS, INAIL, Fondo Previdenza complementare;
 - agli Istituti bancari e finanziari che intrattengono rapporti con la Cassa Edile della Provincia di Napoli;
 - alle Società di servizi, esclusivamente per le finalità della Cassa Edile della Provincia di Napoli;
 - alle Società assicurative;
 - ad altre Casse Edili e loro organismi di coordinamento;
 - agli Enti paritetici di categoria e alla Commissione Nazionale Paritetica per le Casse Edili - Roma;
 - alle Associazioni costituenti la Cassa Edile della Provincia di Napoli;
 - alla Società di revisione contabile;
 - ai Legali e consulenti esterni della Cassa Edile della Provincia di Napoli;
 - alle Associazioni sindacali (nel caso di iscrizione del lavoratore);
 - fornitori di materiale e servizi previdenziali e assistenziali.

PER IL PERSONALE DIPENDENTE DELLA CASSA EDILE:

I dati potranno essere comunicati a:

- tutti i soggetti cui la facoltà di accesso a tali dati è riconosciuta in forza di provvedimenti normativi, ad esempio organi di Polizia e Pubblica Amministrazione in genere;
- ai nostri collaboratori, dipendenti, nell'ambito delle relative mansioni, i quali sono stati e incaricati e autorizzati a trattare i dati forniti;
- a tutte quelle persone fisiche e/o giuridiche, pubbliche e/o private quando la

comunicazione risulti necessaria o funzionale alla costituzione e gestione del rapporto di lavoro, nei modi e per le finalità sopra illustrate, in particolare a:

- Studio Commercialista
- Consulente del lavoro
- Studi Legali
- Istituti bancari
- Istituti Postali
- Istituti previdenziali (INPS, INAIL)
- Fondo Previdenziale (Fondo Prevedi)
- Società di revisione contabile
- Consulente IT
- Società di gestione PEC
- Consulente Privacy
- Compagnie Assicuratrici
- Consulente privacy
- Medico Competente e RSPP per gli adempimenti in materia di sicurezza e salute sul lavoro

PER I FORNITORI (solo se si trattano dati di persone fisiche)

I dati potranno essere comunicati a:

- tutti i soggetti cui la facoltà di accesso a tali dati è riconosciuta in forza di provvedimenti normativi, ad esempio organi di Polizia e Pubblica Amministrazione in genere;
- ai nostri collaboratori, dipendenti, nell'ambito delle relative mansioni, i quali sono stati e incaricati e autorizzati a trattare i dati forniti;
- a tutte quelle persone fisiche e/o giuridiche, pubbliche e/o private quando la comunicazione risulti necessaria o funzionale al corretto adempimento degli obblighi contrattuali e alla gestione della fornitura di beni o servizi, nei modi e per le finalità sopra illustrate, in particolare a:
 - Consulente privacy
 - Studi Commercialisti
 - Consulente del lavoro
 - Istituti bancari
 - Istituti Postali
 - Società di revisione contabile
 - Società di gestione PEC

PER I COMMITTENTI PERSONE FISICHE:

I dati potranno essere comunicati a:

- tutti i soggetti cui la facoltà di accesso a tali dati è riconosciuta in forza di provvedimenti normativi, ad esempio organi di Polizia e Pubblica Amministrazione in genere;
- ai nostri collaboratori, dipendenti, nell'ambito delle relative mansioni, i quali sono stati e incaricati e autorizzati a trattare i dati forniti;
- a tutte quelle persone fisiche e/o giuridiche, pubbliche e/o private quando la comunicazione risulti necessaria o funzionale all'assolvimento dell'obbligo di legge stabilito dall'allegato 17 del D.Lgs 81/08, nei modi e per le finalità sopra illustrate, in particolare a:
 - Società di gestione PEC
 - Fornitore sito web

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.



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.

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.

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.



CRITERI E MODALITÀ DI RIPRISTINO DELLA DISPONIBILITÀ DEI DATI

Il monitoraggio continuo dei dati 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 e vengono poste in essere procedure idonee a garantire l'organizzazione e la custodia della documentazione cartacea gestita dalla Cassa Edile in archivi ad accesso autorizzato e sotto il diretto controllo del Titolare e del DPO.

Si rimanda al capitolo 10 ai fini di una completa descrizione degli archivi cartacei e informatici utilizzati dal titolare del trattamento.



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

9.1 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.

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.



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



Requisiti del sistema informatico

In generale, un sistema informatico 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.



Misure di sicurezza generali

Di seguito sono elencate alcune notazioni riguardo l'adozione delle misure tecniche e organizzative di sicurezza generali.



Misure per trattamenti informatici

- Tutti gli incaricati sono dotati di riconoscimento biometrico delle impronte digitali e 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 Interno al trattamento 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 quotidianamente
- L'evoluzione dei sistemi operativi delle workstation e dei client viene monitorata regolarmente. Gli aggiornamenti tramite patch software sono effettuati con aggiornamenti automatici
- La Cassa tratta i dati relativi allo stato di salute dei propri dipendenti custodendoli in appositi archivi protetti, controllando che ad essi non accedano persone prive di autorizzazione.



Misure per trattamenti cartacei

DOCUMENTO UNICO PRIVACY

- L'ingresso nei locali della Cassa 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 Interno al trattamento della Cassa.
- L'accesso alle stanze archivio è consentito alle sole persone incaricate ed autorizzate a potervi accedere e viene controllato dal Responsabile Interno al trattamento.
- 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 cassette) muniti di serratura e chiusi; l'accesso a tali contenitori è consentito solo alle persone autorizzate a svolgere le operazioni di trattamento.



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	sempre
Parola chiave	Per il trattamento di dati particolari (ex sensibili) e giudiziari deve essere modificata ogni tre mesi	sempre
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	sempre
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

DOCUMENTO UNICO PRIVACY

Profili di autorizzazione	Verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione	sempre
Lista degli incaricati autorizzati	Può essere redatta anche per classi omogenee di incarico	sempre
Antivirus	Efficacia ed aggiornamento sono verificati con cadenza almeno semestrale	ogni giorno
Patch o programmi update	Programmi per elaboratore volti a correggere difetti e prevenire la vulnerabilità degli strumenti elettronici	sempre
Patch o programmi update	Programmi per elaboratore volti a correggere difetti e prevenire la vulnerabilità degli strumenti elettronici (dati particolari - ex sensibili e giudiziari)	sempre
Backup	Salvataggio dei dati con frequenza settimanale	ogni giorno

DOCUMENTO UNICO PRIVACY

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

Descrizione del sistema informatico

La Cassa dispone della seguente architettura hardware:

Nella sala CED troviamo: Server di posta(IBM System X3200) – Server dati(IBM System X3500M4)– Server Proxy (IBM Lenovo ThinkCenter) – Server per nuovo gestionale (HP ML350) - AS400(System i5) con unità a cassette per backup giornaliero. E' presente anche un dispositivo NAS(Western Digital EX4100 MyCloud) dove giornalmente vengono eseguiti i backup dei server. Tutte queste macchine sono sotto ups in una stanza climatizzata chiusa a chiave (sala ced posta al piano terra).

Ci sono 5 fotocopiatrici/stampanti Canon di rete che hanno anche la funzione di fax e scanner.

Al terzo piano è presente una ulteriore stampante di rete a colori Utax P-C3061DN.

La nostra rete è composta da 30 pc windows, ogni pc è dotato di tastiera con riconoscimento biometrico.

Quasi tutti i pc dispongono anche di una stampante laser configurata localmente.

La rete è protetta da un firewall ed un antivirus (McAfee) centralizzati.

Al primo piano è posizionato un mobile rack dove ci sono i collegamenti di rete e telefonici dei vari piani,

gli switch, borchie telefoniche, centralino HP, firewall, router.

DOCUMENTO UNICO PRIVACY

In ogni piano è presente un piccolo mobile rack dove troviamo uno switch di rete e telefonico con relativo ups.

La Cassa dispone della seguente architettura hardware:

Nel rack al primo piano sono collocati:

- 2 Switch MRV MR2228-S2C
- 1 D-Link web smart switch DGS-1210-28
- 1 Firewall Zyxel USG60W
- 1 Router Huawei AR2200 (Linea ADSL principale)
- 1 Router Telecom AGCOMBO (Linea ADSL Backup)
- 2 Net Connect Telefonici
- 1 UPS Riello

Nome server	S.Operativo	DB	Descrizione
Server 1 (Posta)	Windows Server 2003		Server
Server 2	Windows Server 2012 r2	Sql Server 2016	Server
Server Proxy	Ubuntu		Server
AS400	iSeries		Server
Server nuovo gestionale	Windows Server 2016	Sql Server	Server

PC degli Utenti

In azienda sono presenti 30 pc decktop modello Lenovo , intel Core I5, Mem 8Gb, Hd 1000Gb

Tutte le macchine hanno installato come sistema operativo Windows 8

Parco Stampanti

5 Fotocopiatrici Canon modello: IR3245Ne(piano terra) – IR3235N(piano terra) – C5045i(1 piano) – IR3245NE(2 piano) - IR3245(3 piano)

Sono presenti 2 etichettatrici(stampanti termiche) Dymo 450 Turbo

2 Stampanti Triumph Adler modello P3532D

Software Applicativi

Gli applicativi utilizzati in azienda sono i seguenti:

Descrizione	Residente/Gestito	DB
McAfee: Software di Antivirus	Tutti i PC	
Office 365: Sistema di gestione della posta e Suite		
Office 365 Pro Plus	3-Pc	
Acrobat Reader		
Adobe Acrobat 9.0		
7-Zip	Tutti i PC	
Dike		
Durc Client	Su 6 PC	
FileMaker	Su 3 PC	
Color network Scan Gear – Network Scan Gear	Tutti i PC	
SQL Server 2016	Server	
Client Access AS400	Tutti i PC	

Software di base

I software utilizzati per il funzionamento di tutta la struttura informatica, cioè i Sistemi Operativi (S.O.), gli ambienti virtuali (VM) e i Data Base (DB) sono:

Windows Server 2003

Windows Server 2012

Windows Server 2016

Ubuntu 8.04

AS400

Network

Questi sono gli apparati di rete:

- 2 Switch MRV MR2228-S2C
- 1 D-Link web smart switch DGS-1210-28
- 1 Firewall CheckPoint Safe@Office 500

- 1 Router TP-Link TD-W8968 (Linea ADSL principale)
- 1 Router Telecom AGCOMBO (Linea ADSL Backup)

Il locale CED è posizionato in una stanza al piano terra il cui accesso è riservato al personale CED della Cassa Edile Napoli.

Gli apparati di rete sono collocati all'interno di armadio chiuso a chiave sito al primo piano dell'ufficio.

Le chiavi sono a disposizione del personale CED.

Backup

Nel locale CED è previsto un sistema di backup NAS(Western Digital EX4100 MyCloud)

La quantità di dati salvata ammonta a circa 1 Tb. Il salvataggio avviene sullo stesso storage dove sono residenti i dati di produzione. La frequenza di salvataggio è di 1 volta al giorno

Conessioni

La Cassa è servita da un collegamento di Fastweb 100Mb up/ 20 Mb down e una linea adsl di backup di TIM da 20Mb up / 7Mb down.

Centralino

La Cassa dispone di un centralino HP che gestisce telefoni ip

Numeri telefoni IP 31



Rete Locale - Descrizione generale delle caratteristiche del sistema informatico aziendale

I dispositivi informatici utilizzati per il trattamento dei dati della Cassa in qualità di titolare del trattamento sono connessi tra loro attraverso una rete locale Ethernet su protocollo TCP/IP, e si trovano per la maggior parte nel datacenter della Cassa, sito all'interno del locale CED.

La configurazione standard dei client prevede le seguenti configurazioni:

- i client sono membri di dominio, pertanto l'autenticazione è centralizzata in relazione al loro specifico utilizzo (uffici, confezionamento, ecc..)
- è installato software antivirus mantenuto costantemente aggiornato attraverso una procedura automatizzata
- sono installati i software necessari alla corretta operatività aziendale. Periodicamente l'amministratore controlla lo stato del software installato, attraverso un sistema dotato di agent di rilevazione che non effettua monitoraggio dell'attività dell'utente

ma solo dei parametri di configurazione delle macchine, con la finalità di rilevare eventuale software o componenti hardware obsoleti o non autorizzati.

- Non viene effettuato nessun backup dei client, gli utenti sono caldamente invitati a salvare tutto in rete.

Le tipologie dei client sono le seguenti:

- uffici: il client è assegnato univocamente all'incaricato, dotato di credenziali di accesso univoche.



Produzione: i client sono dei pc dove è installato il gestionale, l'accesso a windows avviene in automatico tramite riconoscimento biometrico



Schedari e supporti cartacei

Tutta la documentazione cartacea viene raccolta in schedari, i quali vengono custoditi come segue:

- archivio 1: corrente localizzato presso le postazioni di lavoro presso le scrivanie e appositi armadi nei quali a fine giornata viene riposta tutta la documentazione che è stata utilizzata.
- archivio 2: storico localizzato presso la sede in una stanza dedicata.
- archivio 3: personale localizzato presso la sede dove vengono custoditi i documenti di rilevante importanza costruito con materiale ignifugo. Questo archivio è sempre chiuso e vi hanno accesso soltanto gli incaricati che hanno il compito di gestire tale documentazione.
- archivio 4: corrente localizzato presso la sede nel quale vengono custoditi documenti relativi a dati particolari, per i quali l'accesso è limitato al personale incaricato. Questi documenti vengono gestiti all'interno di una cassaforte ignifuga.



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

DOCUMENTO UNICO PRIVACY

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		60
Inverter per stabilizzazione		X	100
Gruppo elettrogeno		X	100

Presenza dei seguenti dispositivi infrastrutturali

Dispositivo	Si	No	% di locali
Sistema UPS	X		60
Inverter per stabilizzazione		X	100
Gruppo elettrogeno		X	100

Presenza di dispositivi infrastrutturali

Dispositivo	Si	No	% di locali
Armadi ignifughi e stagni	X		2
Quadro elettrico chiuso a chiave	X		
Armadio per i dispositivi di fonia e dati chiuso a chiave	X		
Estintori	X		100

Presenza dei seguenti dispositivi di controllo accessi fisici

DOCUMENTO UNICO PRIVACY

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

La redazione e l'aggiornamento di tale parte del documento unico è stata affidata al Responsabile Progettazione Software della GB SOFT S.r.l.

Sistema informatico Cassa Edile 2000

- caratteristiche tecniche -

Struttura.

Il sistema informatico Cassa Edile 2000 è un prodotto realizzato per la gestione informatica delle Casse Edili, costituito da moduli integrati fra loro.

Tutti i moduli gestionali sono realizzati con i medesimi strumenti di sviluppo software e sono gestiti in un unico database server centralizzato.

Moduli gestionali.

Imprese, operai, cantieri, consulenti, deleghe sindacali, contabilità generale, protocollo generale, gestione banche, interfaccia conti correnti, liquidazioni, prestazioni assistenziali, malattia/infortunio, APE, FNAPE, MUT, BNI, Prevedi, EdilCard, statistiche, elenchi, modulistica, fatture d'acquisto, scadenziario pagamenti, pratiche legali, interfaccia DOL, visure camerali, sistema documentale, invio PEC, portale web imprese e consulenti, portale web legali, servizio SMS operai, app smartphone operai, bollettini bancari.

Strumenti.

Il linguaggio di programmazione utilizzato per la produzione del software gestionale è C++

L'interfaccia per l'accesso di utenti esterni web è realizzata in PHP e Java

Il database server di gestione dei dati è SQL Server

Sicurezza.

Il software gestionale opera nell'ambito della rete locale della Cassa Edile.

Il software gestionale è costituito da un programma eseguibile per ambiente Windows firmato digitalmente dal produttore del software.

Il programma gestionale si avvale di moduli di servizio, sotto forma di programmi eseguibili per ambiente Windows, realizzati dal produttore e firmati digitalmente dal produttore.

La comunicazione fra il programma gestionale ed il database server avviene in rete locale ed è protetta da password di accesso al database.

Ciascun utente viene dotato di una credenziale di accesso (*user-id* e *password*).

La password di accesso è provvisoria e deve essere sostituita dall'utente una volta effettuato il primo accesso al sistema.

È possibile assegnare alle password una durata temporale, altro la quale l'utente dovrà di volta in volta sostituire con una nuova password.

Quando una password è scaduta, l'utente potrà accedere al sistema soltanto dopo aver sostituito la password. L'utente non può riutilizzare password già da egli usate precedentemente.

Gli utenti revocati rimangono memorizzati nel sistema come *inattivi*, per garantire la storia delle rispettive azioni nel sistema.

Gli accessi web di imprese e consulenti avvengono tramite registrazione automatica con codice fiscale ed invio di password di accesso provvisoria all'indirizzo PEC, precedentemente comunicato dall'utente (impresa o consulente delegato) alla Cassa Edile.

Gli accessi web di organi amministrativi della Cassa Edile e consulenti legali avvengono mediante *user-id* e *password* provvisoria (da cambiare al primo accesso) rilasciata direttamente dalla Cassa Edile agli utenti abilitati.

Gli accessi dell'app mobile dei lavoratori avvengono tramite registrazione automatica con codice fiscale ed invio di codice PIN provvisorio via SMS al numero di cellulare del lavoratore, precedentemente comunicato dal lavoratore alla Cassa Edile.

Le comunicazioni via web avvengono in modalità sicura HTTPS / SSL, con crittografia a 128 bit e certificato digitale di autenticità del sito.

Le comunicazioni delle app su smartphone avvengono in modalità sicura REST / HTTPS / SSL, con crittografia a 128 bit e certificato digitale di autenticità del sito.

Gestione profili utenti.

Ciascun utente del sistema gestionale ha un profilo configurabile entro i limiti delle proprie competenze.

Il menù ad albero è personalizzabile. Ogni azione di menù viene associata agli utenti abilitati. Ciascun utente vede il menù con le sole azioni per le quali è abilitato.

Una apposita sezione di personalizzazione del sistema consente di abilitare/disabilitare/nascondere determinate informazioni delle varie videate del sistema, per gruppi di utenti.

Gli elenchi disponibili nelle griglie di visualizzazione sono esportabili in Excel. È possibile abilitare/disabilitare utenti per ciascuna griglia gestita con il programma.

La gestione del menù, delle abilitazioni di dati ed esportazioni Excel può essere messa a disposizione del personale della Cassa Edile addetto alla gestione dei profili utente.

Tracciabilità degli accessi.

Ogni volta che un utente accede al programma gestionale, il sistema trascrive in un apposito registro (log) l'avvenuto accesso o il suo diniego in caso di password errata. Il registro comprende lo user-id utilizzato, la data e l'ora di accesso, l'esito (positivo o negativo), il nome del computer dal quale è stato effettuato l'accesso, il nome dell'utente Windows del computer dal quale è stato effettuato l'accesso. Analogamente, viene registrata la chiusura della sessione quando si chiude il programma.

Registro degli eventi.

Le attività di inserimento, modifica e cancellazione di dati viene tracciata in un apposito registro (log). Di ogni dato inserito, modificato o cancellato vengono tracciati i seguenti dati: Identificativo utente che ha eseguito l'operazione, data ed ora dell'evento, tipo di evento, riferimento al documento e/o al soggetto trattato con l'operazione.

Storico modifiche.

I dati anagrafici di Imprese, Operai e di alcuni tipi di documenti sono sottoposti ad un sistema di tracciabilità che ne memorizza la versione precedente alla modifica e/o alla cancellazione, permettendo, all'occorrenza, di verificare le versioni precedenti dei dati e gli utenti che hanno dato luogo alla modifica.

Aggiornamenti

software.

Gli aggiornamenti rilasciati dal produttore vengono automaticamente scaricati dal server del produttore e si installano automaticamente nel database e quindi nelle postazioni client in modalità automatica, senza alcun intervento manuale da parte degli utenti.

Analogamente, gli aggiornamenti che richiedano modifiche alle strutture dati per la creazione di nuovi campi e strumenti del database vengono eseguiti automaticamente nel database server.

Backup.

Un sistema di salvataggio dei dati, programmato automaticamente nelle ore notturne, produce una copia di backup completa del database gestionale.

Ogni backup vien compresso in modalità .zip ed ha un nome di file costituito dal codice identificativo della Cassa Edile ed il nome del giorno della settimana in cui viene eseguito.

I backup vengono prodotti nel server gestionale. Il personale addetto della Cassa Edile dovrà provvedere a fare una copia del backup, quotidianamente, in un supporto mobile esterno, da portare in una sede diversa da quella del server. I supporti esterni dovranno essere diversi, uno per ogni giorno della settimana, in modo da essere usati a rotazione.

Dietro espressa autorizzazione della Cassa Edile, ogni volta che si esegue un backup, il sistema trasferisce automaticamente la copia di backup, via FTP in modalità sicura, ad un server del produttore del software ospitato in *server farm* di società esterna certificata ISO 27000.

L'archivio documentale, viene registrato in un apposito impianto di *storage* di proprietà della Cassa Edile e dovrà essere salvato periodicamente a cura della stessa.



VALUTAZIONE DEL RISCHIO

FINALITÀ	TIPOLOGIA DI TRATTAMENTO E CONDIZIONE DI LICEITA'	RISCHI SPECIFICI INERENTI I DATI	VALUTAZIONE DEL RISCHIO	MISURE DI SICUREZZA E TIPO DI PROCESSO A CUI I DATI SONO SOTTOPOSTI
Trattamenti per finalità di gestione del personale della Cassa Edile	- Attività di protocollo della documentazione	Perdita	Minimo	- Accessi riservati al solo personale autorizzato
	- Amministrazione gestione del personale	Distruzione	Minimo	- Protezione archivi informatici tramite impronta digitale e parole d'accesso
	- Pagamento stipendi/emolumenti	Divulgazione non autorizzata	Minimo	- Protezione fisica dei documenti inseriti in armadi muniti di serratura, il cui accesso è consentito al solo personale Amministrativo
	- Verifica congruità pagamento delle note spese	Utilizzo improprio	Minimo	- Installazione di un software antivirus e previsione di backup sui server.
	- Assunzioni / collaborazioni / dimissioni / licenziamenti/ trattamenti pensionistici, astensioni obbligatorie e/o facoltative /assistenzialistici /fiscali / assicurativi	Rischio specifico: divulgazione dati aziendali in grado di rivelare inadempienze	Minimo	- Procedura di back up dei dati periodici - Inventario hardware e software

DOCUMENTO UNICO PRIVACY

	<ul style="list-style-type: none"> - Payroll, detrazioni fiscali , trattamenti ex L. 104/1992, esoneri, permessi retribuiti, congedi, etc. - Iscrizione a sindacati (solo per alcuni dipendenti) - Inserimento in Registri cartacei ed elettronici / database necessari per adempiere ad obblighi normativi previsti per tutte le aziende (es. registri professionali, registri INPS, INAIL, etc...) - Rilevazione e normalizzazione delle presenze <p><u>CONDIZIONE DI LICEITÀ È L'ESECUZIONE DEL CONTRATTO CON IL DIPENDENTE DELLA CASSA</u></p>			<ul style="list-style-type: none"> - Aggiornamento annuale dei software e hardware - Estintori in tutto ufficio - Sala server chiusa a chiave con impianto climatizzato accessibile solo dal personale Ced - Non sono presenti antifurti - Accesso ad ogni singolo PC mediante riconoscimento di impronte digitali e password
FINALITÀ	TIPOLOGIA DI TRATTAMENTO E CONDIZIONE DI LICEITA'	RISCHI SPECIFICI INERENTI I DATI	VALUTAZIONE DEL RISCHIO	MISURE DI SICUREZZA E TIPO DI PROCESSO A CUI I DATI SONO SOTTOPOSTI
Formazione del personale della Cassa Edile	<ul style="list-style-type: none"> - Attività di protocollo - Erogazione corsi di formazione interna e anche tramite soggetti esterni - Relazione con soggetti terzi (es. società, enti certificatori che forniscono formazione) <p><u>CONDIZIONE DI LICEITÀ È IL CONTRATTO DI LAVORO CON IL DIPENDENTE E</u></p>	<ul style="list-style-type: none"> Perdita Distruzione Divulgazione non autorizzata Utilizzo improprio Rischio specifico: divulgazione dati aziendali in grado di rivelare inadempienze 	<ul style="list-style-type: none"> Minimo: Minimo Minimo Minimo Minimo 	<ul style="list-style-type: none"> - Accessi riservati al solo personale autorizzato - Protezione archivi informatici tramite impronta digitale e parole d'accesso - Protezione fisica dei documenti inseriti in armadi muniti di serratura, il cui accesso è consentito al solo personale Amministrativo - Installazione di un software antivirus e previsione di backup sui server - Procedura di back up dei dati periodici

DOCUMENTO UNICO PRIVACY

	<u>CONTRATTO DI CONSULENZA PER AGGIORNAMENTI INFORMATICI CON GB SOFT S.R.L.</u>			<ul style="list-style-type: none"> - Inventario hardware e software - Aggiornamento annuale dei software e hardware
FINALITÀ	TIPOLOGIA DI TRATTAMENTO E CONDIZIONE DI LICENZA'	RISCHI SPECIFICI INERENTI I DATI	VALUTAZIONE DEL RISCHIO	MISURE DI SICUREZZA E TIPO DI PROCESSO A CUI I DATI SONO SOTTOPOSTI
Gestione lavoratori iscritti	<ul style="list-style-type: none"> - Attività di protocollo - Liquidazione accantonamenti - Liquidazione A.P.E. (anzianità professionale edile) - Rimborsi malattia/infortunio - Liquidazione prestazioni facoltative - Assistenza e D.P.I. - Servizi di previdenza e mutualità - Corresponsione contributi extracontrattuali - Attività di recupero credito - Corresponsione quote e contributi sindacali - Rimborso Fondo Prevedi - Attuazione accordi collettivi di riferimento - Rilascio della certificazione della regolarità contributiva - MUT con cadenza mensile - iscrizione di un lavoratore ad un Sindacato in seguito a 	<ul style="list-style-type: none"> Perdita Distruzione Divulgazione non autorizzata Utilizzo improprio Rischio specifico: divulgazione dati aziendali in grado di rivelare inadempienze 	<ul style="list-style-type: none"> Massimo Massimo Massimo Massimo Massimo 	<ul style="list-style-type: none"> - Accessi riservati al solo personale autorizzato - Protezione archivi informatici tramite impronta digitale e parole d'accesso -- In Protezione fisica dei documenti inseriti in armadi muniti di serratura, il cui accesso è consentito al solo personale Amministrativo 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 hardware

DOCUMENTO UNICO PRIVACY

	<p>Delega</p> <p><u>- CONDIZIONE DI LICEITA' E' L'APPLICAZIONE DEI CONTRATTI COLLETTIVI NAZIONALI DEL LAVORO SETTORE EDILIZIA (PER LE PRESTAZIONI CONTRATTUALI) E DEL CONTRATTO TERRITORIALE (PER LE PRESTAZIONI EXTRACONTRATTUALI)</u></p>			
FINALITÀ	TIPOLOGIA DI TRATTAMENTO E CONDIZIONE DI LICEITA'	RISCHI SPECIFICI INERENTI I DATI	VALUTAZIONE DEL RISCHIO	MISURE DI SICUREZZA E TIPO DI PROCESSO A CUI I DATI SONO SOTTOPOSTI
Sicurezza (D.Lgs. n. 81/2008)	<ul style="list-style-type: none"> - Attività di protocollo - Visite mediche periodiche al personale dipendente per idoneità alla mansione - Formazione del personale dipendente e non dipendente - Adempimenti di cui al DLgs 81/2008, art. 26 inerenti contratti di appalto con clienti, rischi da interferenza e somministrazione lavoro <p><u>- CONDIZIONE DI LICEITA' E' L'OBBLIGO DI LEGGE (D.LGS. 81/08)</u></p>	<p>Perdita</p> <p>Distruzione</p> <p>Divulgazione non autorizzata</p> <p>Utilizzo improprio</p> <p>Rischio specifico: divulgazione dati aziendali in grado di rivelare inadempienze</p>	<p>Minimo</p> <p>Minimo</p> <p>Minimo</p> <p>Minimo</p> <p>Minimo</p>	<ul style="list-style-type: none"> - Accessi riservati al solo personale autorizzato - Protezione archivi informatici tramite impronta digitale e parole d'accesso - Protezione fisica dei documenti inseriti in armadi muniti di serratura, il cui accesso è consentito al solo personale Amministrativo - 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 hardware
FINALITÀ	TIPOLOGIA DI TRATTAMENTO E CONDIZIONE DI LICEITA'	RISCHI SPECIFICI INERENTI I DATI	VALUTAZIONE DEL RISCHIO	MISURE DI SICUREZZA E TIPO DI PROCESSO A CUI I DATI SONO SOTTOPOSTI
Gestione fornitori (solo se si trattano dati di persone fisiche)	<ul style="list-style-type: none"> - Attività di protocollo - Inserimento in registri / elenchi di fornitori necessari per la gestione del rapporto con 	<p>Perdita</p> <p>Distruzione</p> <p>Divulgazione non autorizzata</p>	<p>Minimo</p> <p>Minimo</p> <p>Minimo</p>	<ul style="list-style-type: none"> - Accessi riservati al solo personale autorizzato - Protezione archivi informatici tramite impronta digitale e

DOCUMENTO UNICO PRIVACY

	<p>fornitore (sistemi informatici gestionali e per la fatturazione,)</p> <ul style="list-style-type: none"> - Gestione rapporto commerciale con fornitore di prodotti o servizi (invio corrispondenza, stipula contratti) - Utilizzo dati per fatturazione/Rapporti commercial <p><u>CONDIZIONE DI LICEITA' E' L'ESECUZIONE DEL CONTRATTO CON IL FORNITORE</u></p>	<p>Utilizzo improprio</p> <p>Rischio specifico: divulgazione dati aziendali in grado di rivelare inadempienze</p>	<p>Minimo</p> <p>Minimo</p>	<p>parole d'accesso</p> <ul style="list-style-type: none"> - Protezione fisica dei documenti inseriti in armadi muniti di serratura, il cui accesso è consentito al solo personale Amministrativo - 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 hardware
FINALITÀ	TIPOLOGIA DI TRATTAMENTO E CONDIZIONE DI LICEITA'	RISCHI SPECIFICI INERENTI I DATI	VALUTAZIONE DEL RISCHIO	MISURE DI SICUREZZA E TIPO DI PROCESSO A CUI I DATI SONO SOTTOPOSTI
Gestione informatica e sicurezza informatica	<ul style="list-style-type: none"> - Attività di protocollo - Gestione autorizzazioni di accesso al sistema informatico e relativa ai profili utente - Gestione delle attività finalizzate ad assicurare l'integrità, la disponibilità e la sicurezza dei dati trattati con mezzi automatizzati - Trattamento dei dati dei dipendenti e dei lavoratori iscritti tramite caselle di posta certificata e mail - Gestione del MUT (software per presentazione telematica delle denunce mensili da parte delle imprese) - App mobile per visualizzare la propria posizione retributiva 	<p>Perdita</p> <p>Distruzione</p> <p>Divulgazione non autorizzata</p> <p>Utilizzo improprio</p> <p>Rischio specifico: divulgazione dati aziendali in grado di rivelare inadempienze</p>	<p>Medio</p> <p>Massimo</p> <p>Massimo</p> <p>Massimo</p> <p>Massimo</p>	<ul style="list-style-type: none"> - Accessi riservati al solo personale autorizzato -- Protezione archivi informatici tramite impronta digitale e parole d'accesso - Protezione fisica dei documenti inseriti in armadi muniti di serratura, il cui accesso è consentito al solo personale Amministrativo - 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 hardware

DOCUMENTO UNICO PRIVACY

	- Accesso area riservata su sito web <u>-CONDIZIONE DI LICEITA' E' IL CONTRATTO DI LAVORO CON IL DIPENDENTE (PER IL CED) E/O IL CONTRATTO DI SERVIZI (PER IL CONSULENTE ESTERNO)</u>			
FINALITÀ	TIPOLOGIA DI TRATTAMENTO E CONDIZIONE DI LICEITA'	RISCHI SPECIFICI INERENTI I DATI	VALUTAZIONE DEL RISCHIO	MISURE DI SICUREZZA E TIPO DI PROCESSO A CUI I DATI SONO SOTTOPOSTI
Notifica preliminare	Comunicazione e gestione del dato dei committenti dei lavori (persone fisiche) ai fini della notifica preliminare <u>- CONDIZIONE DI LICEITA' E' L'OBBLIGO DI LEGGE (ALLEGATO 17 DEL D.LGS 81/08)</u>	Perdita Distruzione Divulgazione non autorizzata Utilizzo improprio Rischio specifico: divulgazione dati aziendali in grado di rivelare inadempienze	ALLO STATO TALE ATTIVITÀ NON VIENE SVOLTA	- Accessi riservati al solo personale autorizzato - Protezione archivi informatici tramite impronta digitale e parole d'accesso - Protezione fisica dei documenti inseriti in archivi cartacei in gestione all'Uff. Amministrativo - 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 hardware

DOCUMENTO UNICO PRIVACY

FINALITÀ	TIPOLOGIA DI TRATTAMENTO E CONDIZIONE DI LICEITA'	RISCHI SPECIFICI INERENTI I DATI	VALUTAZIONE DEL RISCHIO	MISURE DI SICUREZZA E TIPO DI PROCESSO A CUI I DATI SONO SOTTOPOSTI
Gestione Imprese e lavoratori iscritti	<ul style="list-style-type: none"> - Attività di protocollo - Liquidazione accantonamenti - Liquidazione A.P.E. (anzianità professionale edile) - Rimborsi malattia/infortunio - Liquidazione prestazioni facoltative - Assistenza e D.P.I. - Servizi di previdenza e mutualità - Corresponsione contributi extracontrattuali - Attività di recupero credito - Corresponsione quote e contributi sindacali - Rimborso Fondo Prevedi - Attuazione accordi collettivi di riferimento - Rilascio della 	<ul style="list-style-type: none"> Perdita Distruzione Divulgazione non autorizzata Utilizzo improprio Rischio specifico: divulgazione dati aziendali in grado di rivelare inadempienze, il recapito telefonico, email, pec e codice iban -Rischio specifico: divulgazione dati dei lavoratori in grado di rilevare dati particolari come l'adesione al sindacato, le situazioni di malattia e numero di cellulare 	<ul style="list-style-type: none"> Massimo Massimo Massimo Massimo Massimo Massimo 	<ul style="list-style-type: none"> - Accessi riservati al solo personale autorizzato - Protezione archivi informatici tramite identificazione del personale con credenziali personali (utente e password) di accesso fornite dal gruppo direzione - Definizione di profili utente personalizzati per consentire l'accesso di ciascun utente alle funzioni di propria pertinenza - Utilizzazione di un database centralizzato con accesso tramite autenticazione interna alla procedura gestionale -Erogazione servizi web in modalità sicura SSL con crittografia a 128 bit e certificato digitale SSL di autenticità del sito - Distribuzione dati app operai per smartphone tramite VPN e connessione in modalità sicura SSL con crittografia a 128 bit e certificato digitale SSL di autenticità del sito - Installazione antivirus nel

DOCUMENTO UNICO PRIVACY

	<p>certificazione della regolarità contributiva</p> <p>- MUT con cadenza mensile</p> <p>- iscrizione di un lavoratore ad un Sindacato in seguito a Delega</p> <p><u>- CONDIZIONE DI LICEITA' E' L'APPLICAZIONE DEI CONTRATTI COLLETTIVI NAZIONALI DEL LAVORO SETTORE EDILIZIA (PER LE PRESTAZIONI CONTRATTUALI) E DEL CONTRATTO TERRITORIALE (PER LE PRESTAZIONI EXTRACONTRATTUALI)</u></p>			<p>server e nelle postazioni di lavoro con abbonamento ed aggiornamento automatico</p> <p>- Programmazione di backup notturno del database del sistema gestionale con frequenza giornaliera e copie di backup nominate con rotazione settimanale.</p> <p>-Programmazione copia speciale di backup mensile e salvataggio via ftp in modalità sicura</p> <p>-Protezione fisica dei documenti inseriti in archivi cartacei custoditi in depositi il cui accesso è consentito solo al personale amministrativo</p> <p>-Installazione di un software antivirus e previsione di backup sui server</p> <p>-Procedura di backup dei dati periodici</p> <p>-Inventario hardware e software</p> <p>-Aggiornamento annuale dei software e hardware</p>
FINALITÀ	TIPOLOGIA DI TRATTAMENTO E CONDIZIONE DI LICEITA'	RISCHI SPECIFICI INERENTI I DATI	VALUTAZIONE DEL RISCHIO	MISURE DI SICUREZZA E TIPO DI PROCESSO A CUI I DATI SONO SOTTOPOSTI
Gestione fornitori (solo se si trattano dati di persone fisiche)	<p>- Attività di protocollo</p> <p>- Inserimento in registri / elenchi di fornitori necessari per la gestione del rapporto con fornitore (sistemi informatici gestionali e per la fatturazione,)</p> <p>- Gestione rapporto commerciale con fornitore di prodotti o servizi (invio corrispondenza, stipula contratti)</p>	<p>Perdita</p> <p>Distruzione</p> <p>Divulgazione non autorizzata</p> <p>Utilizzo improprio</p>	<p>Medio</p> <p>Medio</p> <p>Medio</p> <p>Medio</p>	<p>- Accessi riservati al solo personale autorizzato</p> <p>- Protezione archivi informatici tramite identificazione del personale con credenziali personali (utente e password) di accesso fornito dal gruppo direzione.</p> <p>- Definizione di profili utente personalizzati per consentire l'accesso di ciascun utente alle funzioni di propria pertinenza</p> <p>Utilizzazione di un database centralizzato con accesso</p>

DOCUMENTO UNICO PRIVACY

	<ul style="list-style-type: none"> - Utilizzo dati per fatturazione/Rapporti commercial <p><u>CONDIZIONE DI LICEITA' E' L'ESECUZIONE DEL CONTRATTO CON IL FORNITORE</u></p>			<p>tramite autenticazione interna alla procedura gestionale</p> <p>Backup ed antivirus trattati nello stesso ambiente gestionale della gestione imprese ed opera iscritti</p>
FINALITÀ	TIPOLOGIA DI TRATTAMENTO E CONDIZIONE DI LICEITA'	RISCHI SPECIFICI INERENTI I DATI	VALUTAZIONE DEL RISCHIO	MISURE DI SICUREZZA E TIPO DI PROCESSO A CUI I DATI SONO SOTTOPOSTI
Gestione informatica e sicurezza informatica	<ul style="list-style-type: none"> - Attività di protocollo - Gestione autorizzazioni di accesso al sistema informatico e relativa ai profili utente - Gestione delle attività finalizzate ad assicurare l'integrità, la disponibilità e la sicurezza dei dati trattati con mezzi automatizzati - Trattamento dei dati dei dipendenti e dei lavoratori iscritti tramite caselle di posta certificata e mail - Gestione del MUT (software per presentazione telematica delle denunce mensili da parte delle imprese) - App mobile per visualizzare la propria posizione retributiva - Accesso area riservata su sito web <p><u>-CONDIZIONE DI LICEITA' E' IL CONTRATTO DI LAVORO CON IL DIPENDENTE (PER IL CED) E/O IL CONTRATTO DI SERVIZI (PER IL CONSULENTE ESTERNO)</u></p>	<p>Perdita</p> <p>Distruzione</p> <p>Divulgazione non autorizzata</p> <p>Utilizzo improprio</p>	<p>Massimo</p> <p>Massimo</p> <p>Massimo</p> <p>Massimo</p>	<ul style="list-style-type: none"> - Accessi riservati al solo personale autorizzato - Protezione archivi informatici tramite identificazione del personale con credenziali personali (utente e password) di accesso fornito dal gruppo direzione. -Definizione di profili utente personalizzati per consentire l'accesso di ciascun utente alle funzioni di propria pertinenza -Utilizzazione di un database centralizzato con accesso tramite autenticazione interna alla procedura gestionale -Backup ed antivirus trattati nello stesso ambiente gestionale della gestione imprese ed opera iscritti



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) il 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 DPO 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 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).

DOCUMENTO UNICO PRIVACY

- 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.