COMUNE DI CASALGRANDE

Piazza Martiri della Libertà, 1 – 42013 Casalgrande (RE)

Tel. 0522 998511 Fax 0522 841039
protocollo@comune.casalgrande.re.it Pec: casalgrande@cert.provincia.re.it
www.comune.casalgrande.re.it Cod. fisc. e P. Iva 00284720356

NORME DI COMPORTAMENTO PER L'UTILIZZO DEGLI STRUMENTI ELETTRONICI E DEI DOCUMENTI CARTACEI DELL'ENTE

ISTRUZIONI OPERATIVE, NORME DI COMPORTAMENTO E LINEE GUIDA PER LA GESTIONE ED IL RISPETTO DEL REGOLAMENTO EUROPEO 2016/679 PER LA PROTEZIONE DEI DATI PERSONALI E LE CORRETTE MODALITA' D'USO DI STRUMENTI DELL'ENTE E CONTROLLI

INDICE

1. SCOPO

Il presente documento ha lo scopo di trasmettere la conoscenza delle modalità operative alle quali i soggetti in generale devono attenersi per garantire il funzionamento del sistema della tutela del "Regolamento Europeo in materia di protezione dei dati personali 2016/679 ", dal D.lgs 196/2003 novellato dal D.lgs 101/2018, delle misure di sicurezza e di impartire delle linee guida per l'utilizzo dei social network e media in ambito personale.

Inoltre il Garante per la protezione dei dati personali, con Provvedimento dell'1.03.2007 pubblicato sulla G. U. R.I. del 10.03.2007, n. 58, ad oggetto "Trattamento di dati personali relativo all'utilizzo di strumenti elettronici da parte dei lavoratori" ha raccomandato l'adozione da parte dei datori di lavoro pubblici e privati (Titolari), di un disciplinare interno, in cui siano indicate le regole per l'uso di Internet, della posta elettronica e della tenuta di file della rete interna. Si fa presente che il Titolare verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle suddette regole pergarantire l'integrità e la tutela del patrimonio dell'Ente, del sistema informatico e la coerenza delle configurazioni e degli archivi con le finalità dell'Ente. Il mancato rispetto di quanto stabilito nel presente regolamento, potrà comportare in capo ad ogni singolo soggetto l'insorgere di:

COMUNE DI CASALGRANDE

Piazza Martiri della Libertà, 1 – 42013 Casalgrande (RE)

Tel. 0522 998511 Fax 0522 841039
protocollo@comune.casalgrande.re.it Pec: casalgrande@cert.provincia.re.it
www.comune.casalgrande.re.it Cod. fisc. e P. Iva 00284720356

- RESPONSABILITÀ PENALE IN CASO DI MANCATA ADOZIONE DELLE MISURE DI SICUREZZA;
- RESPONSABILITÀ CIVILE NEI CONFRONTI DEI TERZI CHE FOSSERO DANNEGGIATI PER EFFETTO DI UN TRATTAMENTO DI DATI NON CORRETTO;
- RESPONSABILITÀ CONTRATTUALE NEI CONFRONTI DEL TITOLARE DEL TRATTAMENTO;
- responsabilità nei confronti dell'Ente con la conseguente possibilità da parte della stessa di contestare il fatto ed applicare i relativi provvedimenti disciplinari previsti dal C.C.N.L. ed in ipotesi di danni economici la richiesta del relativo risarcimento.

2. RIFERIMENTI

Regolamento Europeo in materia di protezione dei dati personali 2016/679– D.lgs 196/2003 novellato dal D.lgs 101/2018 - Provvedimenti e Linee guida del Garante nazionale.
Il riferimento in tema di tutela della libertà e dignità del lavoratore è lo Statuto dei lavoratori – art. 4, Legge 300 del 20/05/1970 come modificato dall'art. 23 del D.lgs. 81 del 23/09/2015.

3. CAMPO DI APPLICAZIONE E DEFINIZIONI

Il presente documento si applica alle modalità di trattamento di tutti i dati personali, al fine di garantire, così come indicato dall'art. 1, 2 e 3 del Regolamento Europeo 2016/679, che il trattamento stesso si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto della protezione dei dati personali.
A tal fine si ricorda che s'intende per:

- **Trattamento:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (Regolamento Europeo 2016/679 art. 4 comma 2);

- **Dato personale**: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (Regolamento Europeo 2016/679 art. 4 comma 1).

- **Dati genetici:** i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione (Regolamento Europeo 2016/679 art. 4 comma 13);
- **Dati biometrici**: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono oconfermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici (Regolamento Europeo 2016/679 art. 4 comma 14);
- **Dati relativi alla salute**: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelino informazioni relative al suo stato di salute (Regolamento Europeo 2016/679 art. 4 comma 15)
- **Dati di categorie particolari:** i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo unico una persona fisica, dati relativa alla salute o alla vista sessuale o all'orientamento sessuale della persona, dati attinenti alla salute fisica o mentale di una persona

(compresa la prestazione di servizi di assistenza sanitaria), che rilevano informazioni relative al suo stato di salute (Regolamento Europeo 2016/679 art. 9 comma 1);

- **Trattamento dei dati personali relative a condanne penali e reati**: i dati personali relativi a condanne penali e reati (Regolamento Europeo 2016/679 Art. 10);
- **Profilazione:** qualsiasi forma di trattamento automatizzato di dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica (Regolamento Europeo 2016/679 art. 4 comma 4).

4. RESPONSABILITA', RUOLI DELLE FIGURE

- **TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI**
- **RESPONSABILI INTERNI (DESIGNATI A SPECIFICHE FUNZIONI)**
- **RESPONSABILE DEL TRATTAMENTO (ESTERNO)**
- **RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI**
- **AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI**
- **AMMINISTRATORE DI SISTEMA**

DEFINIZIONI:

- **Titolare del trattamento:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (Regolamento Europeo 2016/679 art. 4 comma 7);
- **Designati a specifiche funzioni: (Responsabili interni)** Persona autorizzata al trattamento dei dati personali nominato all'interno di ciascuna funzione aziendale per coordinare le attività svolte dagli Addetti all'interno della propria funzione, in merito ad attività con impatto sulla Protezione dei Dati. Tale figura svolge inoltre attività di raccordo tra Soggetti Autorizzati (Regolamento Europeo 2016/679 art. 4 comma 10 – D. Lgs. 196/2003 novellato dal D.Lgs. 101/2018 art. 2 quaterdecies;
- **Responsabile del trattamento (esterno):** la persona fisica, la persona giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (Regolamento Europeo 2016/679 art. 4 comma 8; Art 28);

Responsabile della protezione dei dati personali: figura nominata dal Titolare del trattamento o dal Designato a specifiche funzioni nei casi previsti dal Regolamento Europeo 2016/679 art. 37, che ricopre la posizione prevista dall'art 38 ed i compiti previsti dall'art. 39;**Autorizzati al trattamento dei dati personali:** le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile (Regolamento Europeo 2016/679 art. 4 comma 10 - (Articolo inserito dall'articolo 2, comma 1, lettera f), del D.Lgs. 10 agosto 2018, n. 101);

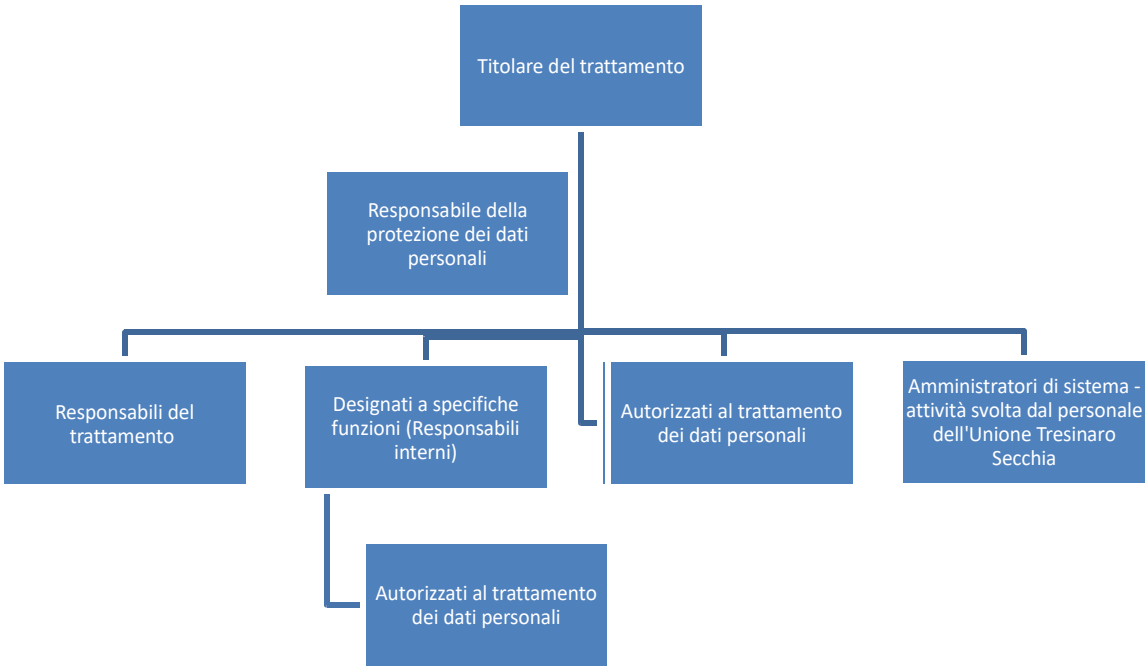
- **Amministratore di sistema:** le figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti (provvedimento del Garante per la protezione dei dati personali datato 27 novembre 2008 - Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore - pubblicato sulla G.U. del 24 dicembre 2008, così come modificato dal successivo provvedimento del 25 Giugno 2009).

Gli aspetti relativi al trattamento dei dati personali sono gestiti dall'Ente in base alla seguente struttura organizzativa:

COMUNE DI CASALGRANDE

Piazza Martiri della Libertà, 1 – 42013 Casalgrande (RE)

Tel. 0522 998511 Fax 0522 841039
protocollo@comune.casalgrande.re.it Pec: casalgrande@cert.provincia.re.it
www.comune.casalgrande.re.it Cod. fisc. e P. Iva 00284720356



Titolare del trattamento dei dati personali

Ogni Ente, quando opera in qualità di Titolare del Trattamento, è responsabile degli obblighi previsti dalla normativa in materia di protezione dei dati personali. In tal senso il Titolare valuta ed adotta tutte le decisioni che riguardano le finalità e i metodi applicati al trattamento dei dati, nonché gli strumenti usati, incluso il profilo e le misure di sicurezza.
In particolare gli obblighi sono:

- adozione delle misure tecniche e organizzative adeguate per garantire, sin dalla fase della progettazione, la tutela dei diritti dell'interessato (privacy by design) e per garantire che i dati non siano persi, alterati, distrutti o comunque trattati illecitamente;

adozione della misure tecniche ed organizzative adeguate per garante che i dati siano trattati, per impostazione predefinita (privacy by default), solo i dati personali necessari per ogni specifica finalità del trattamento;vincolo al dovere di riservatezza dei dati, inteso come dovere di non usare, comunicare o diffondere i dati al di fuori del trattamento;

- designazione del Responsabile del trattamento a cui affidare il trattamento dei dati personali;
- designazione degli addetti al trattamento e degli amministratori di sistemi e vigilare sull'attività degli stessi
- redazione del Registro di trattamenti;
- predisposizione della valutazione d'impatto;
- istruzione del personale;
- documentazione e gestione delle violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio e della eventuale notifica all'Autorità Garante ed ai soggetti interessati.

Il Titolare del Trattamento è costituito dal Legale Rappresentante dell'azienda, espressamente nominato quale rappresentante del Titolare del Trattamento in riferimento alla protezione dei dati personali.

Referente interno per la gestione del Regolamento Europeo 2016/679

I referenti interno privacy sono disponibili all'ind mail privacy@dominioente.re.it, supportato dal consulente CASTGroup Divisione Privacy, dal SIA per la parte informatica.

COMUNE DI CASALGRANDE

Piazza Martiri della Libertà, 1 – 42013 Casalgrande (RE)

Tel. 0522 998511 Fax 0522 841039
protocollo@comune.casalgrande.re.it Pec: casalgrande@cert.provincia.re.it
www.comune.casalgrande.re.it Cod. fisc. e P. Iva 00284720356

Responsabili del trattamento

I terzi che svolgono qualsiasi attività per conto dell'ente che implica il trattamento di dati personali devono essere designati Responsabili del Trattamento o riconosciuti come Titolari autonomi del Trattamento.
Il terzo è Responsabile del Trattamento se non definisce le finalità e i mezzi del trattamento dei dati personali e tratta i dati personali per conto della Ente attenendosi alle istruzioni fornite da quest'ultima.

In caso di mancata designazione a Responsabile del Trattamento dei dati e in assenza di un contratto o altro atto giuridico, il Responsabile può trattare i dati personali soltanto in qualità di Titolare autonomo del Trattamento e l'Ente potrà trasferire i dati personali solo a condizione che esista una specifica condizione di liceità (ad es. consenso dell'Interessato, disposizione di legge, ecc.)
In ogni caso l'Ente deve:

- garantire che il Responsabile del trattamento presenti garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate i modo tale che il trattamento soddisfi i requisiti del GDPR, garantisca la tutela dei diritti degli interessati e rispetti le istruzioni impartite dal Titolare del trattamento;
- avere la possibilità di controllare e vigilare sul trattamento dei dati personali effettuato dal Responsabile del Trattamento.

Il rapporto tra il Titolare del Trattamento e il Responsabile del Trattamento deve essere disciplinata da un contratto o altro atto giuridico e dalla designazione che comprenda, "la materia 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 del Trattamento".
Il documento di nomina deve prevedere inoltre che il Responsabile del Trattamento:
a) tratti 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 informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
c) adotti tutte le misure richieste ai sensi dell'articolo 32;
d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;
e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in 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;
f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e
h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato..

Alla luce di quanto sopra, l'Ente conferirà al terzo l'incarico di Responsabile del Trattamento in base al modello di contratto **utilizzando il documento generato predisposto in forma generica oppure dal portale Privacylab. Il nome del Responsabile del trattamento deve essere inserito nel portale privacylab.**

Tel. 0522 998511 Fax 0522 841039
protocollo@comune.casalgrande.re.it Pec: casalgrande@cert.provincia.re.it
www.comune.casalgrande.re.it Cod. fisc. e P. Iva 00284720356

Designato a specifiche funzioni (Responsabile interno):

I soggetti incaricati alle attività di trattamento (Responsabili interni) nominato all'interno di ciascuna funzione aziendale per coordinare le attività svolte dagli Addetti all'interno della propria funzione, in merito ad attività con impatto sulla Protezione dei Dati. Tale figura svolge inoltre attività di raccordo tra Soggetti Autorizzati : I responsabili interni devono attenersi a quanto previsto nell'atto di designazione e nel documento "**Norme di comportamento per l'utilizzo degli strumenti elettronici e dei documenti cartacei dell'Ente**" consegnato unitamente alla designazione edisponibile nella bacheca aziendale **e** nella bacheca aziendale oltre che alle istruzioni impartite nel presente documento.
La nomina potrà essere revocata nel caso di cambio mansione al dipendente o nel caso di dimissioni/licenziamento.

Addetti designati

I soggetti incaricati delle attività di Trattamento ("**Addetti**") sono le persone fisiche autorizzate, da parte del Titolare del Trattamento, all'esecuzione delle operazioni di trattamento dei dati.
Ogni soggetto che effettua un'attività di trattamento di dati personali, deve essere autorizzato mediante conferimento dell'incarico da parte del Titolare del Trattamento**.** Quanto sopra è da intendersi con riferimento a tutti coloro che accedono ai dati (personale dipendente, somministrato, tirocinanti, stagisti, lavoratori in somministrazione ecc..).
Gli Addetti devono attenersi a quanto previsto nell'atto di designazione e nel documento "**Norme di comportamento per l'utilizzo degli strumenti elettronici e dei documenti cartacei dell'Ente**" consegnato unitamente alla designazione e disponibile nella bacheca aziendale **e** nella bacheca aziendale oltre che alle istruzioni impartite nel presente documento.
La nomina potrà essere revocata nel caso di cambio mansione al dipendente o nel caso di dimissioni/licenziamento.

Amministratori di Sistema

Il Titolare del Trattamento designa gli Amministratori di Sistema che presentano le caratteristiche necessarie per lo svolgimento di tale attività (esperienza professionale, affidabilità, conoscenze teoriche e pratiche per garantire il rispetto della normativa vigente, nonché l'osservanza delle misure di sicurezza)
Gli Amministratori di Sistema , per quanto riguarda i sistemi aziendali, devono assicurare l'adozione delle misure di sicurezza fondamentali prescritte dal GDPR, nonché l'adozione delle misure di sicurezza necessarie per ridurre il rischio che i dati vengano intenzionalmente o accidentalmente distrutti e il rischio di accesso non autorizzato ai dati.
I compiti degli **Amministratori di Sistema** sono esplicitati nella lettera di incarico.
Gli Amministratori di Sistema segnaleranno al Titolare ed al DPO eventuali problemi tecnici riguardanti la raccolta e il trattamento di dati personali, le relative misure di sicurezza che implicano il rischio che i dati vengano intenzionalmente o accidentalmente distrutti o persi, il rischio di accesso non autorizzato ai dati o il rischio di un trattamento eccedente le finalità stabilite per cui i dati sono stati raccolti.

5. MODALITA'

5.1. Trattamento

I dati personali devono essere:
a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non siano incompatibili con tali finalità;c) adeguati, pertinenti e limitati a quanto necessario nel rispetto delle finalità per le quali sono trattati («minimizzazione dei dati»);

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.
f) trattati in maniera da garantirne un'adeguata sicurezza compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati, dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).
Le operazioni di trattamento possono essere finalizzate:
a) alla raccolta
b) al trattamento interno
c) ai rapporti con l'esterno.

In particolare:
a) La raccolta dei dati si riferisce all'acquisizione delle informazioni, direttamente presso l'interessato, presso terzi o mediante la consultazione di elenchi.
b) Il Trattamento interno dei dati consiste nelle operazioni attuate da chi raccoglie le informazioni al fine di organizzarle e renderle utilizzabili.
In particolare:

- la registrazione consiste nell'inserimento dei dati personali in supporti, automatizzati o manuali;
- l'organizzazione si riferisce al trattamento che favorisce l'utilizzo attraverso l'aggregazione o la disaggregazione, l'accorpamento, la catalogazione, ecc.;
- la strutturazione attribuisce significatività ai dati in relazione allo scopo per il quale sono stati raccolti;
- l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione si riferiscono a specifiche operazioni inquadrabili nella fattispecie della strutturazione;
- l'adattamento o la modifica è da porsi in relazione alle variazioni intervenute nei dati dei quali si è già in possesso o all'acquisizione di ulteriori e nuove informazioni;
- il raffronto o l'interconnessione consiste nella messa in relazione tra loro di distinte banche dati per compiere ulteriori trattamenti;
- la conservazione dei dati si riferisce alla loro custodia ed alle conseguenti misure necessarie per garantirne l'aspetto della sicurezza;
- la cancellazione o distruzione dei dati consistente nell'eliminazione degli stessi.

5.2 Protezione dei dati fin dalla progettazione (privacy by design) e protezione per impostazione predefinita (privacy by default)
L'art 25 del Regolamento Europeo 2016/679 prevede che il Titolare del trattamento metta in atto misure tecniche ed organizzative adeguate a soddisfare le necessarie garanzie al fine di soddisfare i requisiti del Regolamento Europeo 2016/679 e che dette misure garantiscono che, per impostazioni predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.
Per maggiore chiarezza si precisa quanto segue:
Protezione dei dati fin dalla progettazione- privacy by design: significa ridurre al minimo il trattamento dei dati personali, mediante misure (tecniche ed organizzative) quali, ad esempio, la*pseudonimizzazione*. In particolare, in fase di sviluppo, progettazione, selezione e utilizzo di applicazioni si deve tenere conto della protezione dei dati personali in modo da assicurarsi che il Titolare del trattamento e i Responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati.
Protezione dei dati per impostazione predefinita – privacy by default: significa adottare misure tecniche ed organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali

necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti , la portata del trattamento, il periodo di conservazione e l'accessibilità.

5.3. Riservatezza e cautela nella comunicazione a terzi di dati e informazioni

Anche informazioni di normale quotidianità dell'Ente o ritenute non riservate all'interno dell'interscambio tra autorizzati, assumono diversa importanza e quindi necessitano di una maggiore tutela, se tali informazioni vengono comunicate all'esterno a soggetti terzi. La salvaguardia delle informazioni e dei dati oltre ad essere un requisito fondamentale per la sicurezza del patrimonio informativo dell'Ente, è anche un espresso obbligo di legge nei confronti di qualsiasi soggetto definito "interessato". A fronte di tali motivazioni è importante ribadire la necessità di osservare ogni cautela nel trasferire all'esterno qualsiasi informazione proporzionalmente al loro contenuto e all'attendibilità dell'interlocutore. Rammentiamo inoltre, che qualora nell'espletamento dell'incarico conferito all'autorizzato, quest'ultimo dovesse, anche accidentalmente o attraverso i colleghi, avere notizia o venire a conoscenza di dati, documenti, informazioni o notizie riguardanti l'organizzazione, l'attività e/o il know-how specifico dell'Ente e dei cittadini che ne fanno parte, queste - fatte salve le notizie o le informazioni che siano o divengano di dominio pubblico - sono da considerarsi oltre che di esclusiva proprietà dell'Ente stesso, anche a carattere assolutamente riservato.

Pertanto, sia nel corso dell'espletamento dell'incarico presso l'Ente, che dopo la scadenza dello stesso, gli autorizzati sono tenuti a mantenere il più rigoroso riserbo sulle suddette informazioni, notizie e dati, ed a non divulgarle o renderle in alcun modo disponibili a terzi, né ad utilizzarle per scopi diversi dai servizi che siete chiamati ad eseguire per conto dell'Ente e del gruppo. E' fatto divieto a tutti gli autorizzati, di conservare, commercializzare, divulgare, trasmettere a terzi in qualsivoglia forma, i dati dell'Ente e dei cittadini che ne fanno parte, a meno che non sia necessario allo svolgimento delle mansioni affidate a ciascun interessato.

5.3.1 Social Engineering

Il social engineering è l'insieme delle tecniche psicologiche usate da chi vuole indurci ai propri scopi presentandosi personalmente presso di noi o contattandoci dall'esterno a mezzo telefono o posta elettronica. Gli obiettivi possono essere quelli della raccolta di informazioni apparentemente innocue riguardanti l'Ente, la sua organizzazione e/o il personale che vi lavora, ma possono arrivare a raggiungere dati anche molto riservati.

Con l'ausilio di messaggi studiati o abili tecniche di persuasione, l'aggressore può anche renderci complici inconsapevoli di azioni che andranno a suo beneficio come, ad esempio: l'acquisizione di informazioni, l'ottenimento della fiducia del personale, l'apertura di allegati infetti e la visita di un sito che contiene dialer o altro materiale pericoloso. Rispetto al social engineering via e-mail, uno dei principali problemi degli autori di virus, è che molti utenti utilizzano strumenti di difesa aggiornati, che non consentono l'esecuzione in automatico di applicativi e quindi non consentono l'attivazione di programmi dannosi. In questo senso l'aggressore potrebbe essere capace di sfruttare i nostri punti di debolezza redigendo abili messaggi che, inducendo fiducia o curiosità, riescono ad arrivare allo scopo.

5.3.2 l'E-mail Phishing

Un altro scopo degli aggressori è indurre l'autorizzato a fidarsi dell'intero contenuto di un messaggio di posta elettronica e quindi ottenere una fedele esecuzione delle istruzioni contenute, ad esempio: vengono inviate false comunicazioni e-mail aventi grafica, forma, autorevolezza e loghi ufficiali di Enti noti, Banche, Intermediari Finanziari, Assicurazioni, ecc., nelle quali si richiedono informazioni attraverso moduli o link a pagine web debitamente camuffate. In questa modalità vengono richieste ad esempio password, numeri di carta di credito o altre informazioni riservate senza che in realtà la raccolta dati abbia nulla a che vedere con l'organismo ufficiale imitato. La vittima crede di comunicare con essi ma in realtà sta trasmettendo informazioni riservate all'aggressore.

Spesso queste tecniche sono abbinate tra loro e applicate più volte nel tempo sulla stessa vittima.

Si elencano di seguito le norme comportamentali:

- non fornire informazioni confidenziali al telefono o di persona a interlocutori non conosciuti;
- fornire informazioni a interlocutori noti e operanti con voi per disposizione del proprio Ente, nei limiti dei contenuti afferenti all'ambito lavorativo a voi assegnato;
- diffidare di messaggi provenienti da fonte non conosciuta;
- non aprire messaggi provenienti da fonte non conosciuta contenenti allegati;
- non aprire messaggi contenenti allegati sospetti;
- non utilizzare mai link contenuti nel testo del messaggio perché possono essere facilmente falsificati: in questi casi si deve andare direttamente sul sito citato digitandone da capo il nome;
- non trasmettere mai alcuna informazione in risposta ad una richiesta proveniente da fonte sconosciuta o non certa come ad esempio: sondaggi telefonici, attività di marketing ecc.;
- non trasmettere mai alcuna informazione in risposta ad una richiesta proveniente da fonti istituzionali o apparentemente conosciute (ad es.: Banche) in quanto tali strutture non richiedono dati utilizzando questa modalità;

Ulteriori informazioni sono rese nell'Allegato "A" predisposto dall'Autorità Garante per la protezione dei dati personali reso in calce al presente documento

6. TRATTAMENTO DEI DATI STRUMENTI ELETTRONICI

6.1 Misure di Sicurezza e comportamenti da tenere

Con il presente documento sono disciplinate altresì le condizioni di utilizzo delle risorse informatiche di archiviazione e di comunicazione che l'Ente mette a disposizione degli autorizzati per l'esecuzione delle funzioni di competenza. Sono inoltre regolate le modalità con le quali l'Ente può accertare e inibire le condotte illecite degli utilizzatori degli apparecchi telefonici, Internet, della posta elettronica e dell'accesso alle risorse di archiviazione di massa (server – hard disk).

Si precisa che l'Ente potrà per necessità di sicurezza di tutela del patrimonio dell'Ente o per esigenze di continuità della normale attività lavorativa, accedere agli strumenti Informatici dati in dotazione ai singoli autorizzati, alle cartelle di rete, ai file di log riservati alla tracciatura degli eventi di connessione (internet), agli archivi di corrispondenza elettronica. Per maggiore chiarezza si dichiara che in caso di necessità l'Ente è in grado di attivare degli strumenti idonei a tracciare le attività di navigazione sulla rete Internet: ovvero per ogni utilizzatore possono essere registrati gli indirizzi dei siti visitati e delle pagine Web consultate. Nel caso della posta elettronica per ogni autorizzato vengono registrati indirizzo mittente, destinatario data/ora invio/ricezione, oggetto del messaggio e l'eventuale presenza di allegati. Per ogni autorizzato di apparecchio telefonico interno vengono registrati i numeri telefonici in uscita. Gli eventuali controlli non saranno effettuati in modalità sistematica né pregiudiziale, ma solo circostanziale e dettate da valutazioni a carattere generale sulla quantità dell'utilizzo dei mezzi e non sul contenuto specifico; controlli puntuali e nel dettaglio dei contenuti specifici saranno effettuati solo in presenza di evidenti abusi e illeciti utilizzi o se richieste dalle forze dell'ordine per controlli e/o provvedimenti giudiziari.

Il S.I.A. (Sistema Informativo Associato) dell'Unione Tresinaro Secchia tuttavia , per ridurre al minimo il rischio di navigazione Internet non consentita, ha optato l'utilizzo di appositi strumenti di filtraggio mediante i quali è stata bloccata la navigazione su categorie di siti i cui contenuti sono stati classificati come certamente estranei agli interessi ed alle attività dell'Ente. Il divieto di accesso a un sito appartenente alle categorie inibite è visualizzato esplicitamente a video.

COMUNE DI CASALGRANDE

Piazza Martiri della Libertà, 1 – 42013 Casalgrande (RE)

Tel. 0522 998511 Fax 0522 841039
protocollo@comune.casalgrande.re.it Pec: casalgrande@cert.provincia.re.it
www.comune.casalgrande.re.it Cod. fisc. e P. Iva 00284720356

6.2 **Personal computer (fisso o portatile), smartphone e tablet, telefono fisso.**
Qualsiasi documento elettronico di qualunque natura o tipo deve essere salvato sui dischi di rete per garantirne il corretto backup;

è altresì fatto espresso DIVIETO a chiunque di memorizzare su dispositivi personali (siano essi pc, smatphone, tablet, ecc.) dati di lavoro con particolare riferimento a quelli della posta elettronica.

Possono tuttavia essere memorizzati su dispositivi aziendali (es. PC fissi o portatili) copie dei dati preventivamente salvati sui dischi di rete.

Tale modalità permette di lavorare in modo flessibile su postazioni differenti permettendo la continuità del servizio in caso di indisponibilità temporanea dello strumento di uso abituale.
Occorre inoltre attnenersi alle seguenti indicazioni:

1. é consentito installare programmi provenienti dall'esterno solo se espressamente autorizzati dal proprio Designato a specifiche funzioni che avrà richiesto autorizzazione al Designato a specifiche funzioni della Sicurezza del S.I.A. (Sistema Informativo Associato);
2. non è consentito scaricare file dalla rete o contenuti in supporti magnetici e/o ottici non aventi alcuna attinenza con lo svolgimento della propria prestazione lavorativa;
3. non è consentito condividere file, cartelle, hard disk o porzioni di questi anche tramite l'uso di Cloud (o similari) che non riguardino espressamente attività richieste per lo svolgimento del proprio lavoro e tanto meno per accedere a servizi non autorizzati al fine di scaricare materiale elettronico tutelato dalle normative sul Diritto d'Autore (software, file audio, film, etc.);
4. i personal computer stand alone o in rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzati per scopi diversi;
5. non è consentito utilizzare il proprio portatile personale in ufficio, se non regolarmente autorizzato dal proprio Designato a specifiche funzioni, che a sua volta dovrà chiedere autorizzazione al Designato a specifiche funzioni del S.I.A.;
6. non è consentito scaricare programmi anche se gratuiti in alternativa a quelli gestiti dall'Ente se non preventivamente concordato con gli Amministratori di Sistema ed autorizzato dal proprio Designato a specifiche funzioni;
7. in caso di cessazione dell'attività lavorativa si precisa che Il S.I.A. (Sistema Informativo Associato) dell'Unione Tresinaro Secchia potrà in ogni momento accedere ai dati che non siano di natura personale, ai back-up dei medesimi dati ed alle cartelle di rete dell'autorizzato dimesso. A tal fine si considera la posta elettronica come dato personale ed, in quanto tale, escluso dall'accesso. L'accesso è effettuato per esigenze lavorative e di verifica sugli strumenti dell'Ente.

6.3 Comportamenti da tenere

Ai fini di cui ai precedenti art. 6.1 e 6.2 sono, quindi, da evitare atti o comportamenti contrastanti con le predette indicazioni come, ad esempio, quelli qui di seguito richiamati a titolo indicativo:

- non è consentito installare software (con licenza o freeware) senza l'autorizzazione del S.I.A. (Sistema Informativo Associato) dell'Unione Tresinaro Secchia.
- non è consentito scaricare software, musica, film ed in generale tutto quando coperto da diritto d'autore, se non preventivamente licenziato;
- non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- è altresì vietato salvare sui pc dell'Ente, cellulari e tablet, foto, documenti (ecc….) di carattere personale. Il PC, lo smartphone e il tablet devono essere utilizzati solo ed esclusivamente per lo svolgimento dell'attività lavorativa;

- non è consentito scaricare file contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa.

LINEE GUIDA PER LA PREVENZIONE DEI VIRUS:

Un virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi. Alcuni virus si limitano a riprodursi senza ulteriori effetti, altri si limitano alla semplice visualizzazionedi messaggi sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido.

Come prevenire i virus:

- Usare soltanto programmi provenienti da fonti fidate: copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato. Non utilizzare programmi non autorizzati, con particolare riferimento ai videogiochi, che sono spesso utilizzati per veicolare virus.
- Attraverso gli amministratori di sistema del S.I.A. verranno mantenuti aggiornati i software antivirus, garantendo la tempestività nell'azione di bonifica, essenziale per limitare i danni che un virus può causare;
- Non diffondere messaggi di dubbia provenienza: è sempre bene diffidare di messaggi che avvisano, ad esempio, di nuovi e pericolosissimi virus. I messaggi e-mail di questo tipo sono detti con terminologia anglosassone hoax (termine che può essere tradotto in italiano con "bufala") e spesso sembrano provenire da un indirizzo di amici, colleghi o comunque da persone conoscenti. Diffidare anche se nel messaggio si fa riferimento a rinomate aziende del settore informatico: spesso frasi come "una notizia proveniente dalla Microsoft" oppure dall'IBM nascondono gli hoax più diffusi.
- Non partecipare a "catene di S. Antonio" o simili: analogamente, tutti i messaggi che vi invitano a "diffondere la notizia quanto più possibile" sono hoax. Anche se parlano della fame nel mondo, della situazione delle donne negli Stati Arabi, di una bambina in fin di vita, anche se promettono guadagni miracolosi o grande fortuna; sono tutti hoax aventi spesso scopi molto simili a quelli dei virus, cioè utilizzare indebitamente le risorse informatiche. Queste attività sono vietate dagli standard di Internet e contribuire alla loro diffusione può portare alla terminazione del proprio accesso.
- Evitare la trasmissione di file eseguibili (.COM, .EXE, .OVL, .OVR) e di sistema (.SYS) tra computer in rete;
- Non utilizzare i server di rete come stazioni di lavoro;
- Non aggiungere mai dati o file Cd, Dvd o chiavette Usb contenenti programmi originali per non violare il copyright sul software;
- Assicurarsi di non eseguire il boot del suo computer da chiavetta Usb, Cd o Dvd. Se il Cd, Dvd o la chiavetta Usb fossero infettati da virus è alta la probabilità che l'infezione si possa trasferirebbe nella memoria RAM e potrebbe espandersi ad altri files;
- Proteggere i propri Cd e/o DVD e/o Chiavette USB da scrittura quando possibile. In questo modo eviterete le scritture accidentali o maliziose di virus e spyware che tentano di propagarsi. I virus non possono in ogni caso aggirare la protezione meccanica;
- Non interrompere in nessun caso le scansioni automatiche dei dispositivi esterni (e.g. chiavetTe USB) che vengono collegate al PC.

6.4 Il S.I.A. (Sistema Informativo Associato) dell'Unione Tresinaro Secchia si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosa per la sicurezza del sistema ovvero acquisiti o installati in violazione delle presenti istruzioni.

Tutti i file di provenienza incerta o esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo e relativa autorizzazione all'utilizza da parte del S.I.A. (Sistema Informativo Associato) dell'Unione Tresinaro Secchia.

COMUNE DI CASALGRANDE

Piazza Martiri della Libertà, 1 – 42013 Casalgrande (RE)

Tel. 0522 998511 Fax 0522 841039
protocollo@comune.casalgrande.re.it Pec: casalgrande@cert.provincia.re.it
www.comune.casalgrande.re.it Cod. fisc. e P. Iva 00284720356

6.5 Utilizzo di connessioni WIFI esterne all'Ente

Se si utilizzano connessioni Wi-Fi esterne messe a disposizione da persone/enti esterni all'Ente (casa, luoghi pubblici, etc..) si ricorda che tali connessioni potrebbero essere non sicure e consentire a persone non identificate di intercettare dati/informazioni trasmessi. Si prega di utilizzare tali servizi solo in caso di assoluta necessità.

6.6 Sistema di autenticazione

Il trattamento di dati personali con strumenti elettronici (pc, tablet e smartphone) da parte dell'Autorizzato è consentito sulla base di credenziali di autenticazione personale.
Tali credenziali di autenticazione consistono:

- PER I PERSONAL COMPUTER, IN UN CODICE PERSONALE (USERNAME/NOME UTENTE) ASSOCIATO AD UNA PASSWORD CONOSCIUTA ESCLUSIVAMENTE DAL SINGOLO AUTORIZZATO.
- PER GLI SMARTPHONE ED I TABLET IN UN PIN CONOSCIUTO ESCLUSIVAMENTE DAL SINGOLO AUTORIZZATO: È VIETATO SALVARE IL PIN IN AUTOMATICO.

6.7 Modalità di elaborare le password

Le credenziali di autenticazione sono assolutamente personali e non cedibili, per alcuna ragione. Se si è in possesso di più credenziali di autenticazione, fare attenzione ad accedere ai dati unicamente con la credenziale relativa al trattamento in oggetto.

Elaborare le password seguendo le istruzioni sotto riportate. Il più semplice metodo per l'accesso illecito a un sistema consiste nell'indovinare la password dell'autorizzato legittimo. In molti casi sono stati procurati seri danni al sistema informativo a causa di un accesso protetto da password "deboli". La scelta di password "forti" è, quindi, parte essenziale della sicurezza informatica.
Cosa non fare

- NON indicare a nessuno la sua password. Ricordare che lo scopo principale per cui si utilizza una password è assicurare che nessun altro possa utilizzare le proprie risorse o possa farlo a proprio nome.
- NON scrivere la password da nessuna parte per evitare che possa essere letta facilmente, soprattutto vicino al computer.
- Quando si immette la password assicurarsi che nessun altro stia guardando la tastiera;
- NON scegliere password che si possano trovare in un dizionario. Su alcuni sistemi è possibile "provare" tutte le password contenute in un dizionario per vedere quale sia quella giusta.• NON credere che l'uso parole straniere possa rendere più difficile il lavoro di scoperta, infatti chi vuole scoprire una password è dotato di molti dizionari delle più svariate lingue.
- NON usare il proprio nome autorizzato. È la password più semplice da indovinare.
- NON usare password che possano in qualche modo essere legate a se stessi come ad esempio: il proprio nome, quello della propria moglie/marito, quello dei propri figli, del proprio cane, la propria data di nascita, i propri numeri di telefono ecc..

cosa fare obbligatoriamente

- La password deve essere composta da almeno 8 caratteri e nel rispetto delle impostazioni degli Amministratori di Sistema del S.I.A. (Sistema Informativo Associato).
- L'autorizzato deve provvedere a modificare la password immediatamente, non appena la riceve per la prima volta, dagli Amministratori di Sistema del S.I.A. (Sistema Informativo Associato).
- La password di posta deve essere modificata dall'autorizzato almeno ogni 3/6 mesi, qualora il sistema non lo richieda automaticamente.
- Si ricorda che per coloro che gestiscono in modo autonomo pc portatili con utenze locali al pc devono provvedere loro stessi alla modifica della password.
- E' obbligatorio collegare i pc portatili alla rete aziendale almeno una volta al mese al fine di permettere l'aggiornamento dei software e dell'antivirus.

Tel. 0522 998511 Fax 0522 841039
protocollo@comune.casalgrande.re.it Pec: casalgrande@cert.provincia.re.it
www.comune.casalgrande.re.it Cod. fisc. e P. Iva 00284720356

Cosa fare praticamente:
Utilizzare più di una parola e creare password lunghe.
A volte è più semplice ricordare una frase completa di senso compiuto piuttosto che una parola complicata e questa tecnica oltre a facilitare la memorizzazione migliora la sicurezza stessa della parola chiave: la lunghezza influisce sulle difficoltà di individuazione e ci consente di utilizzare lo "spazio" tra una parola e l'altra come ulteriore elemento da intercettare.
Inoltre è bene sapere che diversi strumenti di intercettazione presumono che le password non siano formate da più di 14 caratteri, e quindi, anche senza complessità, le password molto lunghe (da 14 a 128 caratteri) possono rappresentare un ottima protezione contro possibili violazioni.
Utilizzare numeri e simboli al posto di caratteri
Non limitarsi alle sole lettere ma, dove possibile, utilizzare l'ampia gamma di minuscole/maiuscole, numeri e simboli a disposizione sulla propria tastiera:
• caratteri minuscoli: a, b, c,...
• caratteri maiuscoli: A, B, C,...
• caratteri numerici: 0,1,2,3,4,5,6,7,8,9.....
• caratteri non alfanumerici: (< > , .) ` ~ ! $ % ^ ; * - + = | \ { @ # } [/] : ; " ' ?.....
Per maggiori informazioni si rimanda all'Allegato "B" "CONSIGILI FLASH PER LA TUTELA DELLA TUA PRIVACY CON BUONE PASSWORD" predisposto dall'Autorità Garante per la protezione dei dati personali consegnato unitamente al presente documento.

6.8 Sistema di autorizzazione
L'ambito del trattamento al quale l'autorizzato è definito dal profilo che gli è stato attribuito sulla base della funzione ricoperta all'interno dell'Ente.

6.9 Utilizzo della postazione di lavoro da parte di utenti diversi
In caso di turnazione sulla stessa postazione di lavoro, l'autorizzato che lascia la postazione di lavoro al collega, deve disconnettersi dalla propria sessione di lavoro, per non lasciare al collega una sessione di lavoro con la propria credenziale di autenticazione (nome autorizzato).Se l'autorizzato che ha lasciato la postazione di lavoro non avesse ottemperato a questa norma, l'autorizzato che subentra deve accede di nuovo alla postazione di lavoro con la propria credenziale di autenticazione.

6.10 Operatività e sicurezza in caso di perdita, distruzione, sottrazione della credenziale di autenticazione
Nel caso di perdita, distruzione, sottrazione, o altro evento che violi la segretezza della credenziale, l'autorizzato deve provvedere alla modifica immediatamente oppure comunicarlo tempestivamente al S.I.A. (Sistema Informativo Associato) dell'Unione Tresinaro Secchia.

6.11 Obbligo di non lasciare incustoditi e accessibili gli strumenti elettronici, mentre è in corso una sessione di lavoro:
Non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento. Lo screensaver automatico con password dopo inattività di 10 o 15 minuti è il miglior strumento per la tutela della riservatezza. È necessario terminare la sessione di lavoro, al computer, ogni volta che ci si deve allontanare anche solo per 5 minuti, effettuando un log out, bloccando il pc oppure mettendo in atto accorgimenti tali, per cui anche in quei 5 minuti il computer non resti:

- incustodito: può essere sufficiente che un collega rimanga nella stanza, durante l'assenza di chi sta lavorando con lo strumento elettronico, anche se la stanza rimane aperta;
- accessibile: può essere sufficiente chiudere a chiave la stanza, dove è situato lo strumento elettronico, durante l'assenza, anche se nella stessa non rimane nessuno.

Tel. 0522 998511 Fax 0522 841039
protocollo@comune.casalgrande.re.it Pec: casalgrande@cert.provincia.re.it
www.comune.casalgrande.re.it Cod. fisc. e P. Iva 00284720356

Non si devono invece mai verificare situazioni in cui, lo strumento elettronico venga lasciato attivo durante una sessione di trattamento, senza che sia controllato da un autorizzato al trattamento o senza che la stanza in cui è ubicato venga chiusa a chiave o senza che lo strumento utilizzato sia privo di screensaver con password.
E' auspicabile installare strumenti software specifici (es.: screensaver) che, trascorso un breve periodo di tempo predeterminato dall'autorizzato in cui l'elaboratore resta inutilizzato, non consente più l'accesso all'elaboratore se non previa imputazione di password. E' cura dell'autorizzato al trattamento verificare l'abilitazione dello strumento con gli Amministratori di Sistema del S.I.A. (Sistema Informativo Associato) dell'Unione Tresinaro Secchia

6.12 Istruzioni aggiuntive in caso di furto e di interruzione del rapporto di lavoro.
In caso di furto o smarrimento di strumenti elettronici o di supporti di identità digitali, l'autorizzato deve avvisare immediatamente il S.I.A. (Sistema Informativo Associato) dell'Unione Tresinaro Secchia (la comunicazione deve essere tempestiva per permettere la chiusura degli accessi dall'esterno e la cancellazione dei dati dal dispositivo mobile) e fare denuncia al più presto ai Carabinieri o alla Polizia Postale, in ragione delle rispettive competenze. Copia della stessa deve essere consegnata alla Direzione del Personale ed al proprio Designato a specifiche funzioni.
In occasione della denuncia di furto o smarrimento occorrerà precisare il contenuto dello strumento elettronico, in particolare se questo contenesse dati personali, accessi a banche dati o quanto possa presupporre un data bridge.

Ulteriori indicazioni operative sono fornite nel punto 11 del presente documento.
In caso di interruzione del rapporto di lavoro, l'autorizzato deve consegnare tutti gli strumenti dell'Ente al S.I.A. (Sistema Informativo Associato) dell'Unione Tresinaro Secchia.

6.13 Norme aggiuntive sull'utilizzo dei device mobili dell'Ente e personali.
Le istruzioni di seguito fornite sono dei suggerimenti non per limitare l'utilizzo dei device, ma si rendono necessarie per garantire un buon livello di salvaguardia delle informazioni e dei dati presenti sui device mobili dell'Ente, con utilizzo esclusivo dell'Ente, e sui device personali (modalità BYOD).

6.13.1 Istruzioni a cui attenersi per gli utilizzatori di device dell'Ente.

1. Il dispositivo viene messo a disposizione dall'Ente per il tempo e l'uso determinato della mansione ricoperta, con l'obbligo di custodirlo con diligenza e renderlo alla cessazione del rapporto, o qualora l'Ente ne faccia richiesta, nello stato originario, fatto salvo il deterioramento fisiologico risultante dall'uso normale dello stesso;
1. Il dispositivo non deve essere lasciato incustodito e/o accessibile a terzi durante una sessione di trattamento. Vietato disattivare il blocco del dispositivo impostato;
2. Il Titolare non è responsabile per il contenuto veicolato attraverso gli strumenti assegnati, né degli usi impropri che ne potrebbero essere fatti;
3. È necessario evitare di installare o utilizzare APP che possano raccogliere dati presenti sul device;
4. È necessario eseguire gli aggiornamenti periodici dei programmi per prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti. Lo strumento è stato impostato per eseguire gli aggiornamenti periodici forniti dal produttore.

6.15 Norme di sicurezza nell'utilizzo dei device mobili dell'Ente
Per evitare i potenziali rischi che derivano dall'utilizzo di tali strumenti, da parte di persone non autorizzate, di seguito alcune misure che l'Ente/Titolare ha individuato e applicato (anche in conformità ex. Art. 32 del REG. Europeo 2016/679)

- Accesso mediante pin;

- Blocco del device sempre attivo;
- Custodia del pin nel rispetto delle necessarie cautele per assicurare la segretezza e la diligente custodia;
- Divieto di utilizzare i dispositivi come hot-spot personale.
- I numeri telefonici lavorativi devono essere salvati di default sulla rubrica della posta elettronica dell'Ente affinché siano salvati con le modalità previste dal Titolare. È ammesso, per semplicità di gestione del dispositivo, salvare con le stesse modalità anche i numeri telefonici personali con la consapevolezza però che la rubrica dell'Ente non è un archivio personale e/o privato.

Il S.I.A. (Sistema Informativo Associato dell'Unione procederà a:

- configurare il telefono cellulare/tablet secondo le esigenze operative e nel rispetto delle misure di sicurezza;
- fornire l'assistenza necessaria al corretto utilizzo del telefono cellulare/tablet;
- gestire le variazioni di attribuzioni a seconda delle variazioni di mansione, e/o richieste da parte della dirigenza;
- curarne tutta la parte infrastrutturale;
- comunicare i limiti di traffico assegnati.

Qualora avvengano incidenti relativi alla sicurezza delle informazioni è necessario avvertire immediatamente il S.I.A. (Sistema Informativo Associato) dell'Unione Tresinaro Secchia di ogni effettivo o sospetto avvenimento di "hacking" e/o rilevazione non autorizzata di dati contenuti all'interno del dispositivo mobile. La tempestiva della comunicazione permetterà al S.I.A. (Sistema Informativo Associato) dell'Unione Tresinaro Secchia di adottare le misure necessarie per la salvaguardia dei dati dell'Ente.

6.15 Device Personali

In generale è espressamente vietato utilizzare dispositivi personali per accedere al sistema informativo dell'Ente ed in particolare per trattare dati.

Eventuali eccezioni devono essere concordate dal Designato a specifiche funzioni e dal S.I.A. (Sistema Informativo Associato) dell'Unione Tresinaro Secchia. In quei casi i dispositivi personali autorizzati devono essere configurati e gestiti con le stesse modalità di quelli della Ente.

6.16 Utilizzo dei supporti removibili

È ammesso il salvataggio dei dati su supporti removibili solo se autorizzati dal S.I.A. (Sistema Informativo Associato) dell'Unione Tresinaro Secchia e dal Designato a specifiche funzioni.

Per coloro che hanno ricevuto l'autorizzazione si ricorda che le modalità di utilizzo sono le seguenti:

- i supporti removibili che contengono dati di qualsiasi natura ivi incluso dati sulla salute, dati particolari, dati relative a condanne penali vanno custoditi con la massima diligenza e in luogo non accessibile da soggetto diverso dall'autorizzato utilizzatore del supporto. A tal fine si ricorda che, in nessun caso, tali supporti possono essere detenuti su scrivanie, scaffalature, cassettiere e armadi privi di serrature, ecc., ma obbligatoriamente custoditi in locali o arredi atti ad evitare i rischi di accessi e trattamenti non autorizzati. (es. cassetti e/ armadi chiusi a chiave);
- i supporti removibili contenenti dati personali (es. CD-ROM, chiavette usb, hard disk esterni ecc.), contenenti dati anche sulla salute, dati particolari e relative a condanne penale e reati, se non utilizzati, non possono essere abbandonati. Devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente non ricostruibili. Le modalità dovranno essere richieste alil S.I.A. (Sistema Informativo Associato) dell'Unione Tresinaro Secchia.

COMUNE DI CASALGRANDE

Piazza Martiri della Libertà, 1 – 42013 Casalgrande (RE)

Tel. 0522 998511 Fax 0522 841039
protocollo@comune.casalgrande.re.it Pec: casalgrande@cert.provincia.re.it
www.comune.casalgrande.re.it Cod. fisc. e P. Iva 00284720356

6.17 Utilizzo della posta elettronica

Per lo svolgimento delle mansioni all'autorizzato al trattamento viene attribuita una casella di posta elettronica dell'Ente che dovrà essere utilizzata per finalità esclusivamente riconducibili allo svolgimento dell'attività lavorativa.

Nel precisare che la posta elettronica è uno strumento di lavoro, si ritiene utile segnalare che:

- dal momento che esiste un dominio di proprietà dell'Ente (@dominioente.it) al quale è collegato un servizio di posta e la relativa casella (es.:mario.rossi@dominioente.it), non è consentito, per fini lavorativi, utilizzare web mail esterni, ovvero caselle di posta elettronica non appartenenti al dominio o ai domini dell'Ente salvo diversa ed esplicita autorizzazione;

- la durata della password è la stessa di dominio (3 mesi).

La "personalizzazione" dell'indirizzo non comporta la proprietà o l'usufrutto in capo all'autorizzato e la liceità dell'utilizzo personale, poiché trattasi di strumento di esclusiva proprietà dell'Ente, messo a disposizione al solo fine dello svolgimento delle proprie mansioni lavorative.

Si ricorda che in caso di assenza improvvisa dell'autorizzato dal posto di lavoro, il S.I.A. (Sistema Informativo Associato) dell'Unione Tresinaro Secchia, qualora indispensabile, potrà attivare l'inoltra copia al collega che svolgerà la mansione lavorativa in sua assenza, previa comunicazione preventiva al titolare della medesima.

In caso di cessazione di attività lavorativa l'Ente provvederà tempestivamente a disattivare l'account dell'Ente .

6.18 Utilizzo di Internet (istruzioni valide anche per i device)

L'autorizzato dei dati e/lavoratore potrà accedere ad Internet solo nei limiti dello svolgimento delle Sue mansioni e si dovrà attenere a quanto segue:

- non è consentito navigare in siti non attinenti allo svolgimento delle mansioni assegnate;

- non è inoltre consentito navigare in siti che possano rivelare una profilazione dell'individuo definita 'particolare' ai sensi del Regolamento Europeo 2016/679: quindi siti la cui navigazione palesi elementi attinenti alla fede religiosa, alle opinioni politiche e sindacali del dipendente o le sue abitudini sessuali;

- non è consentito lo scarico di software non preventivamente autorizzati prelevati da siti Internet;

- non è consentito lo scarico di materiale digitale tutelato dalle normative sul Diritto d'Autore (software, file audio, film, etc.) né attraverso Internet né attraverso servizi di *peer to peer*. Fatto salvo specifiche esigenze di lavoro che richiedano questo tipo di attività.

- è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;

- non è permessa la partecipazione, per motivi non professionali a Forum e giochi in rete pubblica, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (o *nicknames*);

Si ricorda inoltre che qualsiasi attività di Navigazione eseguita tramite la connessione Internet dell'Ente, anche se effettuata tramite la rete dati cellulare sui dispositivi mobili, viene registrata ed attribuita, in caso di violazioni di legge, all'Ente.

Si precisa, quindi, che in questi casi il S.I.A. (Sistema Informativo Associato) dell'Unione Tresinaro Secchia, a tutela dell'Ente, collaborerà attivamente con le Forze dell'Ordine per attribuire la responsabilità di tali comportamenti alle singole persone che ne risponderanno nelle opportune sedi.

Si precisa inoltre che tali regole sono valide anche quando si è connessi utilizzando reti esterne o la connessione dati del proprio Smartphone/Tablet/Modem.

6.19 Assistenza tecnica remota.

Il S.I.A. (Sistema Informativo Associato) dell'Unione Tresinaro Secchia o le persone autorizzate al trattamento da esso nominate possono, qualora richiesto o comunque sia necessario, collegarsi al PC dell'autorizzato sia direttamente sulla postazione di lavoro sia da remoto tramite strumenti Informatici previa autorizzazione dell'autorizzato.

6.20 Stampanti e Fotocopiatrici

Le stampanti e le fotocopiatrici devono essere utilizzate esclusivamente per le attività inerenti al proprio lavoro.

Non è consentito stampare o fotocopiare qualunque documento o flusso dati di tipo personale o comunque non coerente e tanto meno in contrasto con l'attività dell'Ente. Si raccomanda di ritirare tempestivamente i documento stampati sui dispositivi condivisi al fine di garantire la riservatezza e la tutela del dato stampato.

7. TRATTAMENTO SENZA STRUMENTI ELETTRONICI (DOCUMENTI CARTACEI).

Anche Per quanto riguarda il trattamento dei documenti cartacei, l'autorizzato/lavoratore deve rispettare le indicazioni del Titolare del trattamento e dei referenti interni alla gestione della privacy* in merito agli archivi a cui poter accedere e ai documenti che può trattare: non trattare nessun documento al di fuori delle autorizzazioni.

Con queste premesse e con l'obiettivo di assicurare la massima riservatezza sono rilasciate le seguenti istruzioni operative:

- l'Ente ha predisposto luoghi appositi dove conservare i documenti contenenti dati personali; questi le verranno comunicati all'occorrenza come pure eventuali variazione degli stessi; come regola generale Tali documenti non devono essere rimossi se non per effettuare le operazioni di trattamento e solo per il tempo necessario. Al termine dell'elaborazione i documenti riservati devono essere riposti nella posizione designata. I documenti riservati e/o che contengono dati sulla salute e/o particolari e/o relative a condanne penale e reati non devono essere lasciati sulle scrivanie;

- Gli atti e i documenti, una volta presi in carico, contenenti dati personali, non devono essere lasciati liberi di vagare senza controllo ed a tempo indefinito negli uffici, ma occorre controllarli e custodirli, per poi restituirli al termine delle operazioni affidate;

- In caso di affidamento di atti e documenti contenenti dati sulla salute, particolari o relative a condanne penale e reati, il controllo e la custodia devono avvenire in modo tale, che ai dati non accedano persone prive di autorizzazione. A tale fine, è quindi necessario che gli uffici, gli armadi e le cassettiere, ovunque essi si trovino, siano chiusi con serratura, o con altri accorgimenti aventi funzione equivalente, nei quali riporre i documenti contenenti dati sulla salute e/o particolari o relative a condanne penale e reati prima di assentarsi dal posto di lavoro, anche temporaneamente (ad esempio, per recarsi in mensa). In mancanza di tali strumenti farlo presente al Titolare o ai referenti interni della gestione della privacy*. Inoltre l'accesso a tali archivi deve essere consentito alle sole persone autorizzate da specifico e scritto profilo di autorizzazione. I documenti non dovranno mai essere abbandonati ed essere riconsegnarti non appena terminato l'incarico che ne ha determinato il trattamento;

Tel. 0522 998511 Fax 0522 841039
protocollo@comune.casalgrande.re.it Pec: casalgrande@cert.provincia.re.it
www.comune.casalgrande.re.it Cod. fisc. e P. Iva 00284720356

- accertarsi che un visitatore o terzo (o collega autorizzato o non che si intrattiene per troppo tempo) non possa entrare in ufficio anche non invitato (quindi non controllato) e possa venire a conoscenza dei contenuti dei documenti;

- limitare al minimo il numero di fotocopie effettuate (solo se veramente necessario e non in modo ridondante). Tali documenti dovranno essere gestiti con le stesse identiche procedure previste per l'originale;

- i documenti contenenti dati personali non più necessari od inutilizzati non dovranno essere semplicemente cestinati, ma dovranno essere fisicamente resi inutilizzabili da chiunque (es. è vietato cestinare fogli interi o parte di foglio che siano compiutamente leggibili);

- utilizzare una procedura adeguata per la consegna delle copie ai destinatari, tale da fornire sufficienti garanzie di sicurezza (buste sigillate...);
- se i documenti devono essere portati all'esterno del luogo del lavoro, bisogna evitare che soggetti non autorizzati ne possano prendere visione (contenitore chiuso – es busta sigillata- non abbandonare la custodia ...);

- evitare assolutamente di discutere e/o comunicare dati personali per telefono se non si è sufficientemente certi che il corrispondente sia a sua volta autorizzato a venirne a conoscenza;

- effettuare stampe o fotocopie inutili od eccessive senza l'autorizzazione necessaria;

- lasciare incustoditi, o peggio dimenticare, documenti contenenti dati personali nella fotocopiatrice, sul fax, nella stampante , (ecc…);

- sottrarre, cancellare, distruggere senza autorizzazione dati stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento;

- consegnare a persone non autorizzate, senza l'autorizzazione del Titolare pro-tempore del trattamento dei dati, stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

8. CONTROLLO ACCESSI ED ALTRE CREDENZIALI DI AUTORIZZAZIONE (BADGE)

8.1 Controllo accesso ai locali

Gestire l'apertura e la chiusura degli uffici/edifici dove si opera in modo oculato, al fine di prevenire l'accesso e l'utilizzo di strumenti in forma non autorizzata.

8.2 Altre credenziali di autorizzazione (badge)

Il badge assegnato all'autorizzato/lavoratore è strettamente personale e deve essere custodito e conservato con la massima cura. Il badge è necessario per la rilevazione delle presenze.
La rilevazione della presenza deve essere fatta presso il più vicino lettore badge disponibile presso gli uffici o i reparti di assegnazione, prestando attenzione a che il lettore emetta un suono, solo in questo caso infatti, la presenza sarà registrata.

Il badge in dotazione sono in possesso e uso esclusivo di ogni autorizzato ed è severamente vietato e quindi perseguibile, consegnare ad altri il proprio badge per timbrare, per accedere all'ente o per qualunque altro motivo. E' inoltre fatto divieto l'utilizzo di badge di altri autorizzati. In caso di smarrimento o mancanza del badge o danneggiamento dello stesso, l'autorizzato deve immediatamente comunicarlo alla Direzione del Personale. Si afferma che le informazioni ed i dati raccolti tramite il badge/transponder sono utilizzabili a

tutti i fini connessi al rapporto di lavoro, ivi inclusi quelli disciplinari, e saranno oggetto di controllo da parte dell'Ente.
Gli strumenti di rilevazione presenze lavorative non sono strumenti di controllo a distanza ai sensi della normativa vigente. In ragione di ciò (e fermo rimanendo che il dato personale è archiviato e custodito secondo la normativa prevista dal Regolamento Europeo) l'Ente può in ogni momento eseguire dei controlli sul corretto uso degli stessi e del corretto svolgimento della prestazione lavorativa sulla base dei dati raccolti con tali mezzi. I controlli sono eseguiti nel rispetto della massima riservatezza e da personale appositamente autorizzato e formato dal Titolare. I controlli possono essere compiuti attraverso i dati acquisiti dagli strumenti di registrazione degli accessi e delle presenze lavorative.

9. CONTROLLI

9.1 Modalità di svolgimento dei controlli

Nel caso in cui un evento dannoso, fraudolento od una situazione di pericolo, non siano state evitate neppure con i preventivi accorgimenti tecnici e organizzativi sopra indicati, l'Ente potrà adottare misure che consentano la verifica dei comportamenti anomali. In tal senso, gli eventuali controlli, saranno eseguiti nel pieno ed assoluto rispetto di quanto previsto dalla normativa e secondo i principi di "necessità", "correttezza" e non eccedenza.

La prima fase: controlli in forma aggregata ed anonima sulla struttura lavorativa.

In prima battuta, saranno effettuati solo ed esclusivamente controlli preliminari su dati aggregati riferiti all'intera struttura lavorativa. Tali controlli anonimi si concluderanno con un avviso generalizzato all'intera struttura lavorativa in cui si è verificata l'anomalia riferito al rilevato utilizzo anomalo degli strumenti dell'Ente e con l'invito ad attenersi scrupolosamente ai compiti lavorativi assegnati e alle istruzioni contenute nel presente documento.

La seconda fase: controlli in forma aggregata ed anonima sulle aree

In seconda battuta, saranno effettuati solo ed esclusivamente controlli preliminari su dati aggregati riferiti alle sue aree. Tali controlli anonimi si concluderanno con un avviso generalizzato all'intera area in cui si è verificata l'anomalia riferito al rilevato utilizzo anomalo degli strumenti dell'Ente e con l'invito ad attenersi scrupolosamente ai compiti lavorativi assegnati e alle istruzioni contenute nel presente documento.

La terza fase: controlli individuali

Se l'utilizzo anomalo degli strumenti di lavoro dell'Ente assegnati ad esclusivo uso dell'Ente, "Personal computer", "smartphone", "Tablet", "Internet", "Posta Elettronica" e "altri dispositivi", dovesse persistere, si procederà - previa autorizzazione dell'autorità giudiziaria - ad effettuare controlli sull'operato della singolo autorizzato/lavoratore utilizzabili a tutti i fini connessi al rapporto di lavoro, nel rispetto della massima riservatezza e da personale appositamente autorizzato e formato dal Titolare del trattamento.

9.2 Conseguenze a livello giuridico e disciplinare

Come indicato nel punto 6.1 essendo l'Ente ed il singolo autorizzato potenzialmente perseguibile con sanzioni, anche di natura penale, l'Ente verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole, l'integrità del proprio sistema informatico e la coerenza delle sue configurazioni e dei suoi archivi con le finalità dell'Ente (Pc portatile o fisso, smartphone, Tablet, internet, casella di posta elettronica, rete dell'Ente ecc....)
L'Ente, pur nel pieno e costante rispetto della normativa del Regolamento Europeo a tutela del lavoratore, si riserva di segnalare (per obbligo di legge, per tutela propria, dei colleghi di lavoro e dei terzi in genere) alla competente Autorità comportamenti costituenti reato e a condanne penali. Si riserva, altresì, di agire sotto il profilo civilistico/amministrativo/disciplinare in caso di mancato rispetto delle presenti istruzioni, od in presenza di altri tipi di violazione.

COMUNE DI CASALGRANDE

Piazza Martiri della Libertà, 1 – 42013 Casalgrande (RE)

Tel. 0522 998511 Fax 0522 841039
protocollo@comune.casalgrande.re.it Pec: casalgrande@cert.provincia.re.it
www.comune.casalgrande.re.it Cod. fisc. e P. Iva 00284720356

10. LINEE GUIDA PER I DIPENDENTI SUI SOCIAL MEDIA

10.1 Per Social media si intende qualunque sito Web nel quale le persone autorizzate al trattamento dei dati personali/lavoratori sono in grado di condividere contenuti con molti altri visitatori. I contenuti condivisi possono includere informazioni personali, opinioni, commenti, video, foto, informazioni commerciali, ecc. Esempi di tali applicazioni web, sono: Facebook, Twitter, YouTube, LinkedIn…. Anche blog, forum e community sono considerati Social Media. Si ritiene opportuno ricordare alle persone autorizzate al trattamento/lavoratori che la riservatezza deve essere rispettata anche nell'utilizzo personale dei social media in quanto anche l'uso personale dei social media da parte degli persone autorizzate al trattamento/lavoratori ossia al di fuori delle proprie mansioni può arrecare danno all'immagine dell'Ente.
Le persone autorizzate al trattamento/lavoratori sono responsabili dei contenuti che pubblicano nei Social Media, e ne rispondono ai sensi di legge, in sede civile, penale, amministrativa e disciplinare.
Si ricorda che il diritto di critica nei confronti del datore di lavoro (Ente), sia esso esercitato sui Social Media come in qualsiasi altro contesto pubblico, è soggetto a stringenti limiti di veridicità dei fatti e continenza sostanziale e formale. Qualsiasi dichiarazione che comporti una lesione del decoro dell'Ente con eventuale danno d'immagine e relativo danno economico rappresenta un comportamento idoneo a ledere la fiducia che sta alla base del rapporto di lavoro, con violazione del dovere previsto dall'art. 2015 C.C... Tale predetto comportamento può avere rilievo disciplinare e nei casi più gravi costituire presupposto per giusta causa di licenziamento. Di conseguenza qualsiasi comunicazione deve rispettare la politica e l'immagine dell'Ente.
La circolazione delle informazioni inserite nei social media, non è contenibile, né governabile dall'autore. La pubblicazione di dati sui Social Media, è configurabile come operazione di diffusione del dato ai sensi del Regolamento Europeo 2016/679 e pertanto soggetta alla speciale disciplina restrittiva prevista dal Regolamento Europeo stesso. Ricordate che internet non dimentica: tutto ciò che pubblicate resta on-line per molto tempo. Tenetelo sempre presente prima di pubblicare qualcosa.

Quando si pubblicano contenuti (ad esempio foto, filmati, dati…) oppure si inseriscono post o commenti, si ricorda di:

a) attenersi alle norme del Regolamento Europeo 2016/679 e alle istruzioni fornite dall'Ente;
b) attenersi alle norme in tema di copyright e riservatezza dell'Ente;
c) non pubblicare contenuti lesivi per l'immagine dell'Ente;
d) non divulgare o utilizzare informazioni di qualsiasi natura relative all'Ente ed al proprio lavoro svolto per l'Ente;
e) non divulgare o utilizzare foto e/o immagini scattate all'interno dell'Ente;
f) essere consapevoli che verrete associati all'Ente sui Social Media se nel vostro profilo avete specificato di esserne dipendenti. Assicuratevi che il vostro profilo ed i contenuti allegati ad esso, siano coerenti con l'immagine che volete dare di voi.

11. VIOLAZIONE DEI DATI PERSONALI

11.1 Violazione dei dati personali (art. 4.12 – art. 33 e 34 del Regolamento Europeo 2016/679 – Wp 250 Rev01)
La violazione dei dati personali è la "violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".
Si intende per:

- Distruzione: la distruzione dei dati quando gli stessi non esistono più o non esistono più in una forma che sia di qualche utilità per il titolare del trattamento;
- Danno: i dati personali sono stati modificati, corrotti o non sono più completi;
- Perdita: il caso in cui i dati potrebbero comunque esistere, ma il titolare del trattamento potrebbe averne perso il controllo o l'accesso, oppure non averli più in possesso;
- Trattamento non autorizzato o illecito: può includere la divulgazione di dati personali a (o l'accesso da parte di) destinatari non autorizzati a ricevere (o ad accedere a) i dati oppure qualsiasi altra forma di trattamento in violazione del regolamento.

COMUNE DI CASALGRANDE

Piazza Martiri della Libertà, 1 – 42013 Casalgrande (RE)

Tel. 0522 998511 Fax 0522 841039
protocollo@comune.casalgrande.re.it Pec: casalgrande@cert.provincia.re.it
www.comune.casalgrande.re.it Cod. fisc. e P. Iva 00284720356

Si indicano qui di seguito alcune situazioni esemplificative e non esaustive che possono configurarsi come violazione dei dati personali:

- perdita o il furto di un dispositivo contenente una copia della banca dati di soggetti interessati del titolare del trattamento: perdita Chiavetta USB – Laptop- Smartphone o qualunque dispositivo
- il caso in cui l'unica copia di un insieme di dati personali sia stata crittografata da un ransomware (malware del riscatto) oppure dal titolare del trattamento mediante una chiave non più in suo possesso.
- i dati vengono cancellati accidentalmente
- in caso di dati crittografati in maniera sicura, quando la chiave di decifratura viene persa.
- in caso di interruzione significativa del servizio abituale dell'azienda, ad esempio un'interruzione di corrente o attacco da "blocco di servizio" (denial of service) che rende i dati personali indisponibili
- accesso da persone non autorizzate ai dati personali
- dati comunicati a terzi non autorizzati:
- invio di mail a persone non destinatarie del messaggio
- invio di mail in a o in cc anziché in ccn a persone terze non autorizzate (es Una e-mail di marketing diretto viene inviata ai destinatari nei campi "a:" o "cc:", consentendo così a ciascun destinatario di vedere l'indirizzo e-mail di altri destinatari.)
- un soggetto terzo informa il titolare del trattamento di aver ricevuto accidentalmente i dati personali di uno dei suoi clienti e fornisce la prova della divulgazione non autorizzata.
- nel caso in cui sia presente un servizio online e si è subito un attacco informatico con conseguente prelievo di dati personali di tale servizio

Gli addetti, in presenza di una delle situazioni sopra elencate o altre sostituzione non espressamente elencate di analoga natura, devono avvisare immediatamente il Titolare, che valuterà se si tratta di una violazione di dati personali da comunicare all'autorità di controllo competente entro 72 ore dall'averne avuto notizia. Se la notifica non potrà avvenire entro 72 ore, i motivi del ritardo dovranno essere spiegati nella notifica e le informazioni potranno essere rilasciate in fasi successive senza ulteriore indebito ritardo. Il Titolare dovrà valutare l'impatto della violazione

di dati sui diritti e le libertà delle persone fisiche al fine di determinare se sia necessario comunicarla all'autorità di controllo competente e/o all'Interessato. Tale valutazione dovrà essere motivata, documentata e archiviata con il supporto del DPO.

Il Manuale operativo per la gestione delle Violazione dei dati personali è disponibile **nel documento Gestione data Breach in possesso del Titolare e dei referenti interni privacy**

12. AGGIORNAMENTI PERIODICI

Il presente documento sarà aggiornato periodicamente, per adeguarsi all'evoluzione normativa e all'evoluzione tecnologica. E' compito delle persone autorizzate al trattamento/LAVORATORI fare riferimento sempre all'ultima versione

13. REFERENTI DELL'ENTE

In caso di dubbi, esigenze pratiche ed operative, per supporto tecnico hardware e software, su quanto sopra esposto contattare il SIA effettuando una richiesta all'indirizzo http://intranet.unione.ts .

Allegato A) consegnato unitamente al presente documento "IL PHISHING ATTENZIONE AI PESCATORI DI DATI PERSONALI" predisposto dall'Autorità Garante per la protezione dei dati personali
Allegato B) consegnato unitamente al presente documento "CONSIGILI FLASH PER LA TUTELA DELLA TUA PRIVACY CON BUONE PASSWORD" predisposto dall'Autorità Garante per la protezione dei dati personali
Allegato C) consegnato unitamente al presente documento "RANSOMWARE" predisposto dall'Autorità Garante per la protezione dei dati personali.

COMUNE DI CASALGRANDE

Piazza Martiri della Libertà, 1 – 42013 Casalgrande (RE)

Tel. 0522 998511 Fax 0522 841039
protocollo@comune.casalgrande.re.it Pec: casalgrande@cert.provincia.re.it
www.comune.casalgrande.re.it Cod. fisc. e P. Iva 00284720356

Casalgrande, lì _____

_____

COMUNE DI CASALGRANDE.
Il SINDACO
GIUSEPPE DAVIDDI
Titolare del trattamento dei dati personali

COMUNE DI CASALGRANDE

Piazza Martiri della Libertà, 1 – 42013 Casalgrande (RE)

Tel. 0522 998511 Fax 0522 841039
protocollo@comune.casalgrande.re.it Pec: casalgrande@cert.provincia.re.it
www.comune.casalgrande.re.it Cod. fisc. e P. Iva 00284720356

ALLEGATO A

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

IL PHISHING: Attenzione ai «pescatori» di dati personali

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

La truffa avviene di solito via e-mail, ma possono essere utilizzati anche sms, chat e social media. Il «ladro di identità» si presenta, in genere, come un soggetto autorevole (banca, gestore di carte di credito, ente pubblico, ecc.) che invita a fornire dati personali per risolvere particolari problemi tecnici con il conto bancario o con la carta di credito, per accettare cambiamenti contrattuali o offerte promozionali, per gestire la pratica per un rimborso fiscale o una cartella esattoriale, ecc..

In genere, i messaggi di phishing invitano a fornire direttamente i propri dati personali, oppure a cliccare un link che rimanda ad una pagina web dove è presente un *form* da compilare. I dati così carpiti possono poi essere utilizzati per fare acquisti a spese della vittima, prelevare denaro dal suo conto o addirittura per compiere attività illecite utilizzando il suo nome e le sue credenziali.

ALCUNI CONSIGLI PER DIFENDERSI

1. IL BUON SENSO PRIMA DI TUTTO

Dati, codici di accesso e password personali non dovrebbero mai essere comunicati a sconosciuti. E' bene ricordare che, in generale, banche, enti pubblici, aziende e grandi catene di vendita non richiedono informazioni personali attraverso e-mail, sms, social media o chat: quindi, meglio evitare di fornire dati personali, soprattutto di tipo bancario, attraverso tali canali. Se si ricevono messaggi sospetti, è bene non cliccare sui link in essi contenuti e non aprire eventuali allegati, che potrebbero contenere virus o programmi *trojan horse* capaci di prendere il controllo di pc e smartphone. Spesso dietro i nomi di siti apparentemente sicuri o le URL abbreviate che si trovano sui social media si nascondono link a contenuti non sicuri. Una piccola accortezza consigliata è quella di posizionare sempre il puntatore del mouse sui link prima di cliccare: in molti casi si potrà così leggere in basso a sinistra nel browser il vero nome del sito cui si verrà indirizzati.

2. OCCHIO AGLI INDIZI

I messaggi di phishing sono progettati per ingannare e spesso utilizzano imitazioni realistiche dei loghi o addirittura delle pagine web ufficiali di banche, aziende ed enti. Tuttavia, capita spesso che contengano anche grossolani errori grammaticali, di formattazione o di traduzione da altre lingue. E' utile anche prestare attenzione al mittente (che potrebbe avere un nome vistosamente strano o eccentrico) o al suo indirizzo di posta elettronica (che spesso appare un'evidente imitazione di quelli reali). Meglio diffidare dei messaggi con toni intimidatori, che ad esempio contengono minacce di chiusura del conto bancario o di sanzioni se non si risponde immediatamente: possono essere subdole strategie per spingere il destinatario a fornire informazioni personali.

3. PROTEGGERSI MEGLIO

E' utile installare e tenere aggiornato sul pc o sullo smartphone un programma antivirus che protegga anche dal phishing. Programmi e gestori di posta elettronica hanno spesso sistemi di protezione che indirizzano automaticamente nello spam la maggior parte dei messaggi di phishing: è bene controllare che siano attivati e verificarne le impostazioni. Meglio non memorizzare dati personali e codici di accesso nei browser utilizzati per navigare online. In ogni caso, è buona prassi impostare password alfanumeriche complesse, cambiandole spesso e scegliendo credenziali diverse per ogni servizio utilizzato: banca online, e-mail, social network, ecc. *[vedi anche la scheda del Garante con i consigli per gestire le password in sicurezza]*, a meno di disporre di sistemi di autenticazione forte (*strong authentication*).

4. ACQUISTI ONLINE IN SICUREZZA

Se si fanno acquisti online, è più prudente usare carte di credito prepagate o altri sistemi di pagamento che permettono di evitare la condivisione di dati del conto bancario o della carta di credito.

5. LA PRUDENZA NON E' MAI TROPPA

Per proteggere conti bancari e carte di credito è bene controllare spesso le movimentazioni e attivare sistemi di *alert* automatico che avvisano l'utente di ogni operazione effettuata. Nel caso si abbia il dubbio di essere stati vittime di phishing è consigliabile contattare direttamente la banca o il gestore della carta di credito attraverso i canali di comunicazione conosciuti e affidabili.

Per segnalazioni e richieste di ulteriori informazioni: urp@gpdp.it

COMUNE DI CASALGRANDE

Piazza Martiri della Libertà, 1 – 42013 Casalgrande (RE)

Tel. 0522 998511 Fax 0522 841039
protocollo@comune.casalgrande.re.it Pec: casalgrande@cert.provincia.re.it
www.comune.casalgrande.re.it Cod. fisc. e P. Iva 00284720356

ALLEGATO B

www.garanteprivacy.it/flash

1 COME E' FATTA UNA BUONA PASSWORD

Una **buona password**

- deve essere abbastanza **lunga** (almeno 8 caratteri);
- deve contenere **caratteri di almeno 3 diverse tipologie**, da scegliere tra le 4 seguenti: lettere maiuscole, lettere minuscole, numeri, caratteri speciali (punti, trattino, *underscore*, ecc.);
- **non** dovrebbe **contenere riferimenti** personali facili da indovinare (nome, cognome, data di nascita, ecc.);
- **andrebbe periodicamente cambiata**, almeno per i profili più importanti o quelli che usi più spesso (e-mail, *e-banking*, *social network*, ecc.).

Consigli flash

X TUTELARE

la tua privacy

con buone password

2 UTILIZZA PASSWORD DIVERSE PER ACCOUNT DIVERSI (e-mail, *social network*, ecc.)

In caso di «furto» di una password eviterai così il rischio che anche gli altri profili che ti appartengono possano essere violati.

3 CONSERVA CON CURA LE PASSWORD

- **Non conservare mai** le password su biglietti che poi tieni nel portafoglio o indosso, oppure in *file* non protetti su pc, *smartphone* o *tablet*.
- **Evita di condividere** le password via e-mail, sms, *social network*, *instant messaging*, ecc.. Anche se le comunichi a persone conosciute, le credenziali potrebbero essere diffuse involontariamente a terzi o «rubate» da pirati informatici.
- Se usi pc, *smartphone* e altri *device* che non ti appartengono, **evita** che possano **conservare in memoria le password da te utilizzate.**

4 PROVA AD USARE SOFTWARE «GESTORI DI PASSWORD»

Si tratta di programmi specializzati che **generano password sicure** e consentono di **appuntare sul pc tutte le password salvandole in un database cifrato sicuro.**
Ce ne sono di vario tipo, gratuiti o a pagamento.

Ti suggeriamo di consultare anche le altre schede informative che trovi su www.garanteprivacy.it/flash e le nostre campagne di comunicazione «Social privacy», «Fatti smart» e «Connetti la testa».
Se hai dubbi e domande, puoi contattare l'URP del Garante:
www.garanteprivacy.it/home/urp

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

COMUNE DI CASALGRANDE

Piazza Martiri della Libertà, 1 – 42013 Casalgrande (RE)

Tel. 0522 998511 Fax 0522 841039
protocollo@comune.casalgrande.re.it Pec: casalgrande@cert.provincia.re.it
www.comune.casalgrande.re.it Cod. fisc. e P. Iva 00284720356

ALLEGATO C