COMUNE DI BREGANZE

Provincia di Vicenza

PROVVEDIMENTO DEL SINDACO N. 2 DEL 23/02/2022

OGGETTO: NOMINA DIPENDENTI COMUNALI ART 29 GDPR E 2 QUATERDECIES.

IL SINDACO

- Visto il Regolamento UE 2016/679 del Parlamento europeo e del Consiglio datato 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati – di seguito anche RGPD - che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati) entrato in vigore il 25 maggio 2018;
- Visto il D. lgs 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali", così come novellato dal D. lgs. 10 agosto 2018, n. 101 entrato in vigore il 19 settembre 2018;
- Dato atto che ai sensi del Regolamento UE 2016/679 il Comune di Breganze è Titolare dei trattamenti dei dati personali effettuati sia con strumenti elettronici che senza l'ausilio di strumenti elettronici necessari per lo svolgimento dei procedimenti amministrativi afferenti alle funzioni istituzionali affidate dalle fonti di diritto dell'Unione europea e dello Stato italiano ai Comuni;
- Vista la necessità di predisporre adeguate misure per il rispetto e l'adempimento del Regolamento UE 2016/679;
- Preso atto che il Sindaco *pro tempore* rappresenta il Comune nella qualità di titolare del trattamento e ne svolge le relative funzioni;
- Considerato che la normativa europea e quella nazionale pongono a carico del Titolare una serie di obblighi, tra i quali l'attribuzione di funzioni e compiti a soggetti espressamente designati;
- Considerato che ai sensi dell'art. 2-quaterdecies co. 1 D. lgs 196/2003, "*il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità*";
- Considerato che ai sensi dell'art. 2-quaterdecies co. 2 D. lgs. 196/2003, spetta al titolare o al responsabile del trattamento individuare le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta;
- Considerato che ai sensi dell'art. 29 RGPD "*Il Responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del Titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal Titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri*";
- Considerato che l'autorizzazione al trattamento di cui agli artt. 2-quaterdecies D. Lgs. 196/2003 e 29 RGPD può avvenire tramite decreto sindacale;
- Dato atto che i dipendenti di questo Comune sono in grado di offrire garanzie sufficienti in

termini di conoscenza specialistica, esperienza, capacità ed affidabilità per attuare le misure tecniche ed organizzative adeguate a garantire che i trattamenti dei dati personali siano effettuati in conformità al RGPD e ai principi elencati dal presente Decreto, in conformità a quanto espressamente previsto dal Regolamento UE 2016/679;

DISPONE

A) di autorizzare al trattamento ai sensi dell'art. 29 RGPD e dell'art. 2 *quaterdecies* D. lgs. 196/2003 – così come novellato dal D. lgs. 101/2018 – i dipendenti comunali di cui all'allegato 1) al presente decreto **(All. 1)**;
B) di dare atto che l'autorizzazione a tali trattamenti ha durata pari a quello dell'incarico di dipendente comunale conferito.

L'autorizzazione al trattamento affidata con il presente Decreto è relativa ai procedimenti amministrativi, ad iniziativa d'ufficio e di parte, afferenti alle materie concernenti le funzioni istituzionali attribuite a questo Comune dalle fonti di diritto dell'Unione europea e dello Stato italiano, limitatamente ai procedimenti di competenza della struttura cui sono stati assegnati.
I soggetti autorizzati al trattamento ai sensi degli artt. 2-quaterdecies D. Lgs. 196/2003 e 29 RGPD, nel corso del proprio incarico, devono trattare i dati personali rispettando scrupolosamente i compiti e le istruzioni impartite dal Titolare che vengono fornite in allegato **(All. 2).**

Il presente Decreto dovrà essere:
- consegnato a mani proprie o via mail ai Responsabili di P.O e ai dipendenti comunali;
- comunicato al Responsabile della protezione dei dati;
- pubblicato nella sezione "amministrazione trasparente" del sito web istituzionale di questo Comune.

Si allega al presente decreto:
Allegato 1: Elenco dipendenti comunali
Allegato 2: Istruzioni per Addetti al trattamento ai sensi del Regolamento UE 2016/679 e D. Lgs. 196/2003 come modificato dal D. Lgs. 101/2018

Breganze, 23 Febbraio 2022

COMUNE DI BREGANZE (Vicenza)

Il Sindaco
Avv. Piera Campana

All. 1 provvedimento Sindaco n. 2.

COMUNE DI BREGANZE

Provincia di Vicenza

Elenco dipendenti Comunali

Cognome	Nome
Acqua	Monica
Benetti	Martina
Borin	Maddalena
Brazzale	Mauro
Broccardo	Lorenzo
Cantele	Maria Paola
Cattelan	Lucio
Covolo	Sergio
Dalla Ricca	Marta
Dalla Stella	Marta
De Fina	Nadia
Franzan	Matteo
Gasparon	Marta
Guzzo	Nicola
Guzzonato	Alessandra
Lain	Gianluca
Maino	Silvia
Manea	Simona
Merlo	Adriano
Michelon	Bertilla
Miotti	Alessandra
Mocellin	Romina
Nardon	Maria
Pavan	Renzo
Pigato	Gilberto
Pigato	Rita Paola
Polga	Mino
Rodighiero	Paola
Rossi	Paola
Seganfreddo	Davide
Seganfreddo	Laura
Seganfreddo	Roberto
Stefani	Cristina
Tedeschi	Caterina
Valerio	Claudio
Zamberlan	Riccardo
Zanin	Andrea
Zanini	Anna Maria

COMUNE DI BREGANZE

Provincia di Vicenza

ISTRUZIONI PER ADDETTI AL TRATTAMENTO AI SENSI DEL REGOLAMENTO UE 2016/679 E D. LGS. 196/2003 COME MODIFICATO DAL D. LGS. 101/2018

Istruzioni a cui sono tenuti ad attenersi gli addetti rispetto al trattamento dei dati personali effettuati per conto del Comune.

Sommario

1. INTRODUZIONE 2
2. AFFIDAMENTO DI DOCUMENTI CONTENENTI DATI PERSONALI 3
2.1. Trattamento senza l'ausilio di strumenti elettronici 3
2.2. Trattamento con l'ausilio di strumenti elettronici 4
3. UTILIZZO DEGLI STRUMENTI DI PROTEZIONE DEI SISTEMI INFORMATICI 8
4. OBBLIGO DI RISERVATEZZA 9
5. PROCEDURE PER IL SALVATAGGIO DEI DATI 10
6. ISTRUZIONI GENERICHE 11

1. INTRODUZIONE

L'Art.29 Regolamento UE 2016/679 – di seguito anche GDPR - definisce come "addetto" il soggetto che agisce sotto l'autorità del titolare del trattamento ovvero del responsabile del trattamento. L'art. 2 quaterdecies D. lgs. 196/2003, come modificato dal D. Lgs. 101/2018, prevede, al co. 1, che "*il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità*".

Il titolare del trattamento è individuato dall'art. 4 n. 7 GDPR come "*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 [..]*"

Il responsabile del trattamento è, ai sensi dell'art. 28 GDPR, il soggetto che effettua un trattamento di dati personali per conto del titolare.

Per trattamento si intende, secondo quanto disposto dall'art. 4 n. 2 GDPR, "*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*".

Nell'ambito di competenza a lei assegnato nella nomina dal titolare, le vengono impartite le istruzioni a cui è tenuto ad attenersi nel trattamento di dati personali, in conformità alla normativa vigente in tema di protezione dei dati personali.

Lei, in qualità di addetto al trattamento dei dati personali, deve essere in grado di individuare il tipo di dato che sta trattando secondo quanto stabilito dalla normativa e, qualora non fosse in grado di farlo, dovrà fare riferimento al titolare del trattamento.
A tal fine, riportiamo di seguito le definizioni e i riferimenti normativi per una più chiara comprensione:

- *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;

- *dati appartenenti a categorie particolari di dati personali* (art. 9 GDPR): dati personali che rilevano origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesti a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
- *dati genetici*: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- *dati biometrici*: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- *dati relativi alla salute*: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

2. AFFIDAMENTO DI DOCUMENTI CONTENENTI DATI PERSONALI

2.1. Trattamento senza l'ausilio di strumenti elettronici.

Lei potrà trattare soltanto i documenti per i quali è stato autorizzato, secondo le indicazioni che le saranno fornite dal Titolare del trattamento.

Custodia. Una volta presi in carico, gli atti e i documenti contenenti dati personali devono essere sempre custoditi e controllati. Concluse le operazioni da compiere, devono essere ricollocati negli appositi archivi. Essi, quindi, non devono essere lasciati a tempo indefinito presso gli uffici o al di fuori di essi. Al termine dell'attività quotidiana devono essere riposti negli appositi archivi.

Qualora le vengano affidati atti e documenti contenenti i cd. "*dati particolari*" di cui all'art. 9 GDPR ovvero i cd. "*dati giudiziari*" di cui all'art. 10 GDPR, il controllo e la custodia devono essere tali da impedire l'accesso a tali dati da parte di soggetti privi di autorizzazione. A tale fine, quindi, in caso di assenza dal posto di lavoro, anche temporanea (p.e.: pausa pranzo), è necessario utilizzare i cassetti muniti di serratura - ovvero adottare altri comportamenti che tendano allo stesso risultato - nei quali riporre i documenti contenenti dati sensibili o giudiziari. Qualora vi fosse la mancanza di tali strumenti, è pregato di sollecitare il titolare, ovvero il responsabile, affinché possa provvedere.

Lei è inoltre tenuto ad assicurare l'accesso a tali archivi alle sole persone autorizzate con specifica nomina, ricordando loro di non abbandonare tali documenti e di riconsegnarli al termine dell'incarico.

Comunicazione. I dati personali di cui può venire a conoscenza durante le attività lavorative non devono essere comunicati a soggetti esterni ovvero a soggetti interni al Comune per i quali non è necessario conoscere tali informazioni.

Distruzione. Qualora fosse necessario distruggere i documenti contenenti dati personali, è opportuno utilizzare gli strumenti "distruggi documenti". Qualora non vi fossero, si raccomanda di distruggere manualmente il documento in modo che non possa più essere ricomposto.

2.2. Trattamento con l'ausilio di strumenti elettronici

I sistemi informatici del Comune. Il PC (fisso o mobile) ed i relativi programmi e/o applicazioni affidati al dipendente sono strumenti di lavoro che necessitano di essere custoditi in modo appropriato e possono essere utilizzati solo per le finalità attinenti all'attività lavorativa, in relazione alle mansioni assegnate, e non per scopi personali.
Il Titolare, ovvero il Responsabile Interno, verificherà, nei limiti consentiti dalla legge e dal contratto, il rispetto delle istruzioni fornite, potendo accedere, sempre nel rispetto della legge, agli archivi ed ai file log relativi ai singoli PC.
L'eventuale smarrimento, furto, danneggiamento deve essere prontamente segnalato al Responsabile interno e/o al Titolare.

Utilizzo del PC. Per quanto riguarda l'utilizzo dei PC, il Comune avvisa che:

a) è consentito installare programmi provenienti da fonti esterne solo su espressa autorizzazione del Titolare del trattamento; non è consentito scaricare file dalla rete o contenuti in supporti magnetici e/o ottici non strettamente riferibili alla prestazione lavorativa;
b) non è consentito utilizzare strumenti software e/o hardware idonei ad intercettare alterare o distruggere il contenuto di comunicazioni e/o documenti informatici; non è consentita l'installazione sul proprio PC di mezzi di comunicazione propri (p.e. modem);
c) non è consentito diffondere in rete, mediante condivisione, i documenti del proprio PC;
d) Salvo espressa autorizzazione del Titolare, non è consentito effettuare il download di materiale elettronico tutelato dalle normative sul Diritto d'autore (software, file audio, film, etc.);
e) i PC stand-alone in rete sono aree di condivisione di informazioni strettamente professionali e non possono essere utilizzate per scopi diversi. Qualunque file non attinente all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità; il Comune si riserva la

facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema ovvero acquisiti o installati in violazione delle presenti istruzioni.

Custodia ed utilizzo dei supporti rimovibili, contenenti dati personali. I supporti rimovibili (es. chiavetta usb) contenenti dati personali riferibili alle categorie particolari di dati personali ai sensi dell'art. 9 GDPR ovvero di dati personali relativi a condanne penali e reati ai sensi dell'art. 10 GDPR o giudiziari devono essere custoditi ed utilizzati in modo tale da impedire accessi non autorizzati e trattamenti non consentiti. Si raccomanda di conservarli in cassetti chiusi a chiave e, una volta terminato il loro utilizzo, procedere alla formattazione ovvero, se necessario, alla distruzione.

Utilizzo di Internet. Per quanto riguarda l'utilizzo di Internet, il Comune l'avvisa che:

a) non è consentito navigare e registrarsi a siti non attinenti allo svolgimento dell'attività lavorativa, in siti vietati dalla legge, con contenuti contrari alla morale ed al buon costume ovvero in siti non attinenti alle prescrizioni impartite dal titolare;
b) non è consentita, salvo autorizzazione del Titolare, effettuare transazioni finanziarie online, di qualsiasi tipo (p.e.: operazioni di *home banking*), acquisti on-line e simili;
c) non è inoltre consentito navigare in siti che possano consentire una profilazione dell'individuo relativa a dati 'particolari' ai sensi dell'art. 9 Regolamento UE 2016/679. Sono da evitare siti la cui navigazione possa rilevare elementi attinenti alla fede religiosa, alle opinioni politiche e sindacali del dipendente ovvero il suo orientamento sessuale;
d) non è consentito effettuare il download, salva espressa autorizzazione del Titolare, di software gratuiti, anche se soltanto di prova, prelevati da siti Internet; non è consentito scaricare il materiale elettronico tutelato dalle normative sul Diritto d'autore (software, file audio, film, etc.) né attraverso Internet né attraverso servizi di P2P, salvo diversa autorizzazione da parte del titolare;
e) non è permessa la partecipazione durante l'orario di lavoro, per motivi non attinenti all'attività lavorativa, a chat, forum, giochi online o simili;
f) non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per motivi relativi all'orientamento sessuale, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

Utilizzo della posta elettronica. La posta elettronica è uno strumento di lavoro e come tale deve essere utilizzato.

In riferimento al suo utilizzo, si forniscono le seguenti indicazioni:

a) salvo autorizzazione da parte del Titolare, non è consentito utilizzare la posta elettronica (interna ed esterna) per motivi non attinenti allo svolgimento delle mansioni assegnate (p.e. per partecipare a chat, forum ovvero per iscriversi a mailing list o servizi di newsletter);

b) non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria nei confronti di altri soggetti per motivi di orientamento sessuale, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
c) salvo autorizzazione da parte del Titolare, non utilizzare la posta elettronica per inviare all'esterno informazioni, dati o documenti di lavoro "strettamente riservati";
d) nel caso esista un dominio di proprietà del Comune al quale sia collegato un servizio di posta e la relativa casella (dipendente@nomecomune.it), non è consentito utilizzare web mail esterni, ovvero caselle di posta elettronica non appartenenti al dominio comunale salvo diversa ed esplicita autorizzazione.

Utilizzo del telefono. Qualora vi fosse la necessità di fornire delle informazioni a mezzo telefono, potrebbe essere necessario, a seconda della tipologia di dati richiesti, chiedere l'identità del chiamante e la motivazione della richiesta prima di dare risposta. Si confronti con il Titolare qualora fossero richiesti dati appartenenti alle categorie di dati particolari di cui all'art. 9 Regolamento UE 2016/679 o dati cd. "giudiziari" di cui all'art. 10 Regolamento UE 2016/679.

Utilizzo del fax.

a) Controlli sempre di aver digitato correttamente il numero di telefono a cui deve essere inviata la documentazione;
b) Qualora dovessero essere trasmessi dati particolari di cui all'art. 9 GDPR ovvero dati cd. "giudiziari" di cui all'art. 10 GDPR, si raccomanda di anticipare l'invio del fax chiamando direttamente il soggetto destinatario così da assicurarsi che il documento sia ricevuto da questi e non da soggetti estranei. Si raccomanda inoltre di effettuare una telefonata di conferma per assicurarsi la corretta ricezione e leggibilità del contenuto del fax.

Custodia. Non lasci incustodito e accessibile lo strumento elettronico durante una sessione di trattamento. È necessario terminare la sessione di lavoro ogni volta che si allontana dal pc, anche se per breve tempo. Questo per evitare che il pc resti, durante la sua assenza, incustodito o accessibile a terzi. Per evitare ciò è sufficiente che, in sua assenza, un suo collega rimanga nella stanza ovvero, qualora non rimanesse nessuno, questa sia chiusa a chiave.
Lo strumento elettronico non deve essere lasciato attivo, durante una sessione di trattamento, senza che sia controllato da un addetto al trattamento ovvero da un Responsabile Interno o senza che la stanza in cui sia ubicato venga chiusa a chiave.
È consigliato installare strumenti software specifici, come lo screen-saver, che, trascorso un breve periodo di tempo predeterminato dall'utente in cui l'elaboratore resta inutilizzato, non consente più l'accesso

all'elaboratore se non previo inserimento della password. Verifichi con il Titolare le possibilità di abilitazione dello strumento.

Modalità per l'elaborazione e la custodia delle credenziali di autenticazione. Le credenziali di autenticazione sono composte da un codice per l'identificazione dell'interessato (*User-id*) associato ad una parola chiave (*password*), oppure in un dispositivo di autenticazione (p.e. *token*) o in una caratteristica biometrica. Queste sono assolutamente personali e non cedibili.

Cosa fare

a) In linea generale, lei è tenuto a rispettare l'ambito di competenza – ossia i dati a cui è autorizzato ad accedere - ed il profilo di autorizzazione – ossia il tipo di trattamento che è autorizzato a compiere - indicate nella propria Nomina ad Addetto;

b) la *password* deve essere composta da almeno otto caratteri, salvo diverse istruzioni. Qualora il sistema non accettasse una *password* di otto caratteri, essa deve essere composta da un numero di caratteri pari a quello massimo consentito dal sistema. Si consiglia di comporre la *password* in modo tale che, di questi caratteri, da un quarto alla metà siano di natura numerica;

c) Utilizzare più di una parola e creare *password* lunghe. Diversi strumenti di intercettazione presumono che le *password* non siano formate da più di 14 caratteri, e quindi, anche senza complessità, quelle molto lunghe – con un numero di caratteri superiore a 14 - possono rappresentare una valida protezione contro possibili violazioni. Si tenga presente, tuttavia, che non tutti i *software* sono in grado di accettare *password* superiori a 14 caratteri.

d) Non scegliere *password* con parole che possano essere trovate in un dizionario, né in quello italiano o di altre lingue. Su alcuni sistemi è possibile "provare" tutte le password contenute in un dizionario per vedere quale sia quella giusta.

e) Non utilizzare parole che possano essere riferibili alla sua persona, come il nome, cognome, data di nascita, nome del figlio, ovvero l'*user-id.*

f) Utilizzare numeri e simboli al posto di caratteri. Ove possibile, deve utilizzare lettere minuscole (a, b, c ...) e maiuscole (A, B, C ...), numeri (0, 1, 2...) e caratteri non alfanumerici (< > , .) ` ~ ! $ %^ ; * - + = | \ { @ # } [/] : ; " '? Non inserisca i numeri e/o i caratteri non alfanumerici alla fine ovvero all'inizio di una parola nota (p.e."123armadio") perché nonostante la lunghezza, tale *password* può essere identificata abbastanza facilmente. Per rendere più complessa la *password*, alcune lettere possono essere sostituite con simboli e numeri. P.E.: invece di "123armadio", inserire "1du&tr€@rmad1()". Cercare di realizzare password utilizzando caratteri appartenenti a tutti i gruppi indicati in precedenza (lettere minuscole e maiuscole, numeri e caratteri non alfanumerici).

g) Qualora all'interno del Comune vi fosse la figura del custode delle copie delle credenziali, è necessario trascrivere una copia della propria parola chiave e consegnarla in busta chiusa sigillata all'addetto ovvero al responsabile incaricato alla loro custodia;

h) Fare riferimento al Titolare per i dettagli operativi della procedura;

i) Deve provvedere a modificare la password immediatamente, non appena ricevuta per la prima volta, da chi amministra il sistema;

j) La *password* deve essere modificata dall'addetto almeno ogni sei mesi; qualora il trattamento riguardi dati particolari *ex* art. 9 GDPR ovvero dati giudiziari *ex* art. 10 GDPR, essa deve essere modificata almeno ogni tre mesi;

k) Mantenere la *password* riservata e non divulgarla a terzi;

l) Non trascrivere la *password* su fogli, post-it o diari;

m) Non immetta la *password* quando è in presenza di altre persone o comunque si assicuri che queste non la stiano guardando mentre la inserisce;

n) Qualora, per la tipologia di trattamento, lei fosse in possesso di più credenziali di autenticazione, dovrà accedere con quella relativa al trattamento in oggetto.

3. UTILIZZO DEGLI STRUMENTI DI PROTEZIONE DEI SISTEMI INFORMATICI

Sono necessari alcuni accorgimenti e misure di sicurezza al fine di evitare danneggiamenti al sistema informatico a causa di virus, *malware* o simili.

Il Titolare e/o il Responsabile, con la collaborazione dell'addetto, dovrà provvedere ad aggiornare con cadenza almeno mensile gli antivirus installati sulla sua postazione PC ed installare le *patch* di aggiornamento dei sistemi operativi e dei programmi utilizzati per il trattamento dati personali, con cadenza annuale e, nel caso di trattamenti di dati particolari di cui all'art. 9 GDPR ovvero giudiziari di cui all'art. 10 GDPR con cadenza almeno semestrale.

Come prevenire i virus.

1. Utilizzare soltanto programmi provenienti da fonti fidate. Ogni programma deve essere sottoposto alla scansione prima di essere installato;
2. Si assicuri che il suo PC sia stato controllato dall'antivirus – che deve essere costantemente aggiornato almeno una volta alla settimana - e provveda a lanciare una scansione dell'intero sistema con il suo software antivirus – se possibile, anche programmandone l'esecuzione automatica;
3. Non diffonda messaggi di dubbia provenienza. Se riceve messaggi, anche da parte di importanti aziende informatiche, che avvisano di un nuovo virus pericoloso, lo ignori: le mail di questo tipo sono "*hoax*" (bufale);

4. Non partecipare a "catene di S. Antonio" o simili. In genere sono veicoli per virus. Queste attività sono vietate dagli standard di Internet e contribuire alla loro diffusione può portare alla terminazione del proprio accesso;
5. Evitare la trasmissione di file eseguibili (.COM, .EXE, .OVL, .OVR) e di sistema (.SYS) tra computer in rete;
6. Non utilizzare i server di rete come stazioni di lavoro;
7. Non aggiungere mai dati o file a memorie di massa removibili ameno che non siano proteggibili in scrittura e con sistema di accesso controllato:
8. Assicurarsi di non dare esecuzione accidentalmente al suo pc da dischetto. Infatti, se il dischetto fosse infettato, il virus si trasferirebbe nella memoria e potrebbe espandersi ad altri *files.*
9. Proteggere i suoi dischetti da scrittura quando possibile. In questo modo eviterete le scritture accidentali, magari tentate da un virus che tenta di propagarsi. I virus non possono in ogni caso aggirare la protezione meccanica.
10. Non utilizzare memorie di massa contenenti dati Personali su altro PC e non in condizioni di protezione in scrittura. Se si utilizza un PC che necessita di essere avviato tramite memoria di massa rimovibile, assicurarsi che non contenga dati personali.
11. Verificare all'inserimento su computer di memorie di massa rimovibili l'eventuale presenza di virus e *malware* con verifica automatica o manuale;
12. Salvo espressa autorizzazione del titolare, non utilizzi supporti di memorizzazione già adoperati in precedenza senza apposito controllo del sistema di antivirus in uso;
13. Salvo espressa autorizzazione del titolare, non utilizzi software gratuiti prelevati da siti Internet o in allegato a riviste o libri;
14. Salvo espressa autorizzazione del titolare, non si colleghi ad Internet con download di file eseguibili o documenti di testo da siti web o da siti FTP; con attivazione degli applets di Java o altri contenuti attivi;
15. Salvo espressa autorizzazione del titolare, ovvero del Responsabile interno, non scarichi allegati non sicuri dalla posta elettronica.

4. OBBLIGO DI RISERVATEZZA

Le informazioni a cui quotidianamente ha accesso nell'ambito delle mansioni svolte, non devono essere comunicate a soggetti esterni. La salvaguardia delle informazioni e dei dati oltre ad essere un requisito fondamentale per la sicurezza del patrimonio informativo comunale, 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.

Presti particolare attenzione alle tecniche di cd. "*social engineering*" ed a quelle di "*e-mail phishing*".

Le prime sono tecniche persuasive rivolte a spingere le persone a fornire – personalmente o a mezzo di e-mail e cellulare - informazioni personali come credenziali di accesso ad un pc al fine di raccogliere informazioni sul Comune, la sua organizzazione ovvero dati personali trattati da questa.

Nel caso in cui venga contattato da sconosciuti, ovvero riceva messaggi anche da parte di aziende informatiche, istituti bancari, assistenziali assicurativi, che richiedano user-id, password, pin o comunque credenziali di accesso ed autenticazione, non dia nessun tipo di riscontro alle richieste e contatti immediatamente il titolare ovvero il responsabile.

Le seconde consistono in una tipologia di frode ideata con lo scopo di rubare informazioni personali, anche di particolare importanza quali dati relativi al conto bancario.

Avviene ad esempio attraverso un messaggio di posta elettronica finalizzato ad 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, chiedendo 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.

Cosa fare:

a) non fornire informazioni confidenziali al telefono o di persona a interlocutori non conosciuti e quando si rivolge a persone note si limiti a quanto strettamente necessario per le finalità lavorative;
b) diffidi di messaggi provenienti da fonte non conosciuta e non apra gli allegati sospetti;
c) non utilizzi 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;
d) non trasmetta mai alcuna informazione in risposta ad una richiesta proveniente da fonte sconosciuta ovvero in risposta ad una richiesta proveniente da fonti istituzionali apparentemente conosciute (ad es.: banche) in quanto tali strutture non richiedono mai dati utilizzando questa modalità;
e) in caso di dubbio è sempre preferibile verificare l'attendibilità delle richieste con il Responsabile o il Titolare.

5. PROCEDURE PER IL SALVATAGGIO DEI DATI.

Gli Addetti sono tenuti a fare riferimento alla politica interna di back up per le istruzioni specifiche di salvataggio. Se è nominato l'Addetto delle copie di *back-up*, egli sarà il referente per tali operazioni.

6. ISTRUZIONI GENERICHE

L'addetto dovrà:

a) procedere alla raccolta di dati personali, nelle modalità previste dalle sue mansioni e secondo quanto indicato dal Titolare.

b) trattare i dati personali nella misura necessaria e sufficiente alle finalità proprie della banca dati nella quale vengono inseriti, secondo quanto espresso nell'informativa e, comunque, in modo lecito e secondo correttezza;

c) adottare, nel trattamento dei dati, tutte le misure di sicurezza ex art. 32 Regolamento UE 2016/679 che siano indicate dal Titolare, in particolare dovrà:

1) per le banche dati informatiche, procedere con l'identificazione mediante *User-ID* e *password*, evitando, così come indicato in precedenza, di operare su terminali di altri e/o di lasciare aperto il sistema operativo con le proprie credenziali inserite in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
2) trattare i soli dati la cui conoscenza sia necessaria e sufficiente per lo svolgimento delle operazioni da effettuare rispettando strettamente il proprio profilo di autorizzazione;
3) conservare i supporti informatici e/o cartacei contenenti i dati personali come descritto nelle istruzioni di cui sopra;
4) copie di dati personali su supporti rimovibili sono permesse solo se effettuate secondo quanto prescritto nelle presenti istruzioni. In ogni caso tali supporti devono avere un'etichetta che li identifichi e non devono mai essere lasciati incustoditi;
5) Qualora vi sia una violazione dei dati personali, l'addetto dovrà comunicarla immediatamente al Titolare, ovvero al Responsabile interno, così da consentire l'eventuale notifica dai sensi dell'art. 33 Regolamento UE 2016/679 ovvero la comunicazione ai sensi dell'art. 34 Regolamento UE 2016/679;
6) segnalare al Titolare eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
7) fornire al Titolare, dietro sua richiesta, tutte le informazioni relative all'attività svolta, al fine di consentirgli di attuare l'attività di controllo sulla protezione dei dati personali;
8) collaborare con il Titolare e gli eventuali Responsabili ex art. 28 Regolamento UE 2016/679 e gli altri addetti ex art. 29 Regolamento UE 2016/679 e art. 2 quaterdecies D. lgs. 196/2003 e s.m.i. alla corretta protezione dei dati personali secondo quanto disciplinato dalla normativa vigente.

d) Aggiornarsi sulle misure di sicurezza in relazione ai profili della disciplina sulla protezione dei dati personali, i rischi attinenti al loro trattamento e le misure disponibili per prevenire eventi dannosi.

Breganze, 23 febbraio 2022

Avv. Piera Campana

Il sottoscritto _____, per presa visione delle "istruzioni per l'addetto" ai sensi dell'art. 29 del Regolamento UE 2016/679 e dell'art. 2-quaterdecies del D. lgs. 196/2003 come modificato dal D. lgs. 101/2018.

Data e luogo

Firma leggibile

Allegato 2 Provvedimento Sindaco n.2-2022