COMUNE DI ALA
Provincia di Trento

Autorizzazione al Trattamento dei Dati

ai sensi dell'art. 2 quaterdecies del d.lgs 196/2003 novellato dal d.lgs 101/2018

Mansioni ed Istruzioni

Il Comune di Ala nella persona del sindaco pro tempore in qualità di Titolare del trattamento dati visto l'art. 2 quaterdecies del D.lgs 196/2003 novellato dal D.lgs 101/2018, considerando che, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento., con la presente

Autorizza

al Trattamento dei Dati

Prescrizioni generali

Cosa sono i dati personali

"Il nuovo regolamento intende come dato personale qualsiasi informazione riguardante una persona fisica identificata o identificabile, si considera identificabile la persona 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".

Le persone fisiche possono essere associate ad **identificativi on line** prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli **indirizzi IP**, marcatori temporanei (**cookies**), o identificativi di altro tipo, come i **tag di identificazione a radiofrequenza**. Tali identificativi possono lasciare tracce che, in particolare, se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone e identificarle.

Categorie "particolari" di dati personali

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 univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. In particolare:

- **dati genetici** 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** 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** 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;

I dati giudiziari

I dati personali che rivelano l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (quali, *ad es.*, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione).

Cosa è il trattamento dei dati personali

Il GDPR definisce trattamento dei dati personali "qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati".
E' quindi indifferente che le operazioni vengano svolte con o senza l'ausilio di mezzi elettronici, o comunque automatizzati, per cui anche i trattamenti effettuati su supporto cartaceo sono assoggettati al regolamento.

Mansionario relativo al trattamento dei dati

a) Istruzioni operative generali

L'incaricato deve effettuare le operazioni di trattamento, che gli vengono affidate, nel rispetto delle disposizioni di legge, verificando in particolare che ai soggetti interessati sia stata data l'informativa pertinente allo specifico trattamento effettuato, che la stessa sia completa in tutte le sue parti e redatta ai sensi dell'art.13 del GDPR.
Nell'ambito della prescrizione generale, l'incaricato, coerentemente con quanto previsto dall'art. 5 del GDPR, deve trattare i dati secondo **liceità, correttezza e trasparenza**, accedendo esclusivamente alle banche dati e ai dati personali **necessari e pertinenti** allo svolgimento dei compiti che gli sono stati affidati e solo per scopi determinati e legittimi non eccedenti le sue mansioni (cosiddetto principio della minimizzazione dei dati).
L'incaricato, inoltre, nell'eseguire le operazioni di trattamento deve rispettare le istruzioni di seguito specificate.
Cautele da seguire per la corretta comunicazione di dati a soggetti terzi o comunque con strumenti impersonali o che non consentono un controllo effettivo dell'identità del chiamante:
- **controllo dell'identità del richiedente:** nel caso di richieste di comunicazione di dati (presentate per telefono o per fax) occorre verificare l'identità del soggetto richiedente, ad esempio formulando una serie di quesiti; in altri casi, può essere utile comunicare all'interessato un codice personale identificativo, da comunicare al personale per ogni comunicazione impersonale (ad esempio a mezzo telefonico);
- **verifica dell'esattezza dei dati comunicati:** nell'accogliere una richiesta di comunicazione di dati personali, da parte dell'interessato ovvero di un terzo a ciò delegato, occorre fare attenzione all'esattezza del dato che viene comunicato, in particolare quando la richiesta viene soddisfatta telefonicamente o attraverso trascrizione da parte dell'operatore, di quanto visualizzato sul monitor.

b) Ambito del trattamento consentito

L'incaricato deve gestire i seguenti archivi e trattamenti:

COMMISSIONE DI CONCORSO

Trattamenti	Finalità
Gestione dei dati personali dei candidati relativi alla procedura di concorso pubblico/selezione pubblica/ progressione interna assegnata	Interesse istituzionale ed esercizio dei pubblici poteri

I dati trattati, necessari per lo svolgimento delle mansioni lavorative, sono custoditi negli archivi, posti negli armadi degli uffici preposti. Tali archivi sono ad accesso selezionato, per cui potrà accedervi nei limiti in cui ciò sia strettamente necessario per prelevare e riporre i documenti necessari per lo svolgimento delle mansioni lavorative.

c) Trattamento con strumenti elettronici

Nello svolgimento dei suoi compiti, all'incaricato potrebbe essere concessa l'autorizzazione all'utilizzo di strumentazione elettronica nella disponibilità del Titolare, in tal caso l'incaricato è autorizzato ad accedere all'elaboratore preposto al trattamento dei dati, previa verifica della sua identità. A tale fine:

- Dovrà utilizzare un codice di identificazione (*username)*
- Dovrà utilizzare una parola chiave (*password*), composta di almeno otto caratteri alfanumerici che dovrà essere modificata almeno ogni sei mesi, nel caso in cui con l'elaboratore tratti solo dati di natura comune, o almeno ogni tre mesi, nel caso in cui con l'elaboratore tratti anche dati di natura particolare o giudiziaria.

La parola chiave:

- deve essere mantenuta segreta, adottando gli opportuni accorgimenti per la sua custodia;
- non deve contenere riferimenti agevolmente riconducibile alla sua persona e dovrebbe essere generata preferibilmente senza un significato compiuto;
- deve essere composta da caratteri speciali e lettere maiuscole e minuscole;

- non deve essere rivelata al telefono, né inviata via fax o e –mail o tramite cellulare, nessuno è autorizzato a richiederla

In particolare l'incaricato dovrà:

- utilizzare la credenziale di autenticazione, composta da Username e Password, provvedere a custodirla con la massima attenzione e segretezza, non divulgarla o comunicarla a terzi nel rispetto di quanto previsto dal GDPR;
- modificare la credenziale di autenticazione ogni volta che dovessero sorgere dei dubbi sulla sua segretezza;
- informare tempestivamente il Titolare del trattamento in caso di situazioni critiche dalle quali potrebbero verificarsi perdite o danneggiamenti dei dati trattati;
- impedire l'accesso non autorizzato ai dati provvedendo, nel caso di assenza anche momentanea dalla postazione di lavoro a chiudere preventivamente tutte le applicazioni in uso sul proprio elaboratore, oppure a porre la macchina in posizione di *stand-by,* adottando un sistema di oscuramento (cd. ***screen-saver***) dotato di password, o ancora a spegnere l'elaboratore che si sta utilizzando;
- per l'accesso a software e portali potrebbero essere previste ulteriori password, che devono seguire, in mancanza di ulteriori indicazioni o vincoli, le indicazioni sopra riportate;
- utilizzare i mezzi informatici, inclusa la posta elettronica (fornita dall'Azienda) e Internet, esclusivamente per scopi aziendali;
- non utilizzare a fini aziendali, a meno che ciò non sia permesso dal Titolare del trattamento o in caso di emergenza, la casella di posta elettronica personale a fini aziendali questo vale sia per web-mail che per caselle POP configurate su Outlook;
- non effettuare download di file o software, senza previa autorizzazione;
- non accedere a dati il cui contenuto sia dubbio o illecito né trasferirli nella rete del Titolare;
- impiegare sui PC solo software provvisti di licenza, acquistati dal Titolare;
- salvare i dati ed i file allegati ai messaggi di posta elettronica, negli archivi aziendali, secondo i criteri di archiviazione definiti;
- non salvare localmente (su disco "C") dati personali su PC collegati in rete, ma salvarli regolarmente su disco di rete con accesso vincolato;
- non accedere a servizi non consentiti; nel caso in cui fosse necessario per la propria attività di usufruire di tali servizi confrontarsi con l'Amministratore di Sistema;
- non caricare ed eseguire software di rete o di comunicazione, senza previa verifica dello stesso da parte dell'Amministratore di sistema;
- non collegare dispositivi che consentano un accesso, non controllabile, ad apparati della rete del Titolare;
- custodire in luogo sicuro i dispositivi rimovibili (es. chiavette usb) contenenti dati personali. Prima di rottamare un qualsiasi dispositivo informatico (compresi i supporti rimovibili) l'incaricato deve cancellare eventuali dati personali contenuti nel dispositivo;
- procedere alla cancellazione dei supporti magnetici od ottici contenenti dati personali, prima che i medesimi siano riutilizzati. Se ciò non è possibile, essi devono esser distrutti;
- nel caso in cui utilizzi dispositivi propri dovrà attenersi ad ulteriori misure di sicurezza, indicate dal Titolare del trattamento o da un suo delegato;
- in caso di furto, danneggiamento o perdita, anche accidentale dei dati o l'accesso abusivo agli strumenti a disposizione (anche personali) contenti dati aziendali dovrà comunicarlo immediatamente al Titolare in modo che possa attivare le procedure di **Data Breach**.

CRM e Banche dati

La visione dei dati; contenuti nelle banche dati, **esclude** comunque qualsiasi forma di comunicazione, diffusione e trattamento degli stessi che non sia strettamente funzionale all'espletamento dei compiti e che non si svolga nei limiti stabiliti da leggi e regolamenti

d) Utilizzo dei byod (Bring your own device – porta il tuo dispositivo) se permessi

Qualora un incaricato sia stato espressamente autorizzato dal Comune all'utilizzo di dispositivi elettronici personali durante le attività lavorative, premesso che il Comune è "Titolare del trattamento" relativamente ai dati che sono trattati per suo conto da parte dell'incaricato al trattamento, occorre che si uniformi alle sottostanti prescrizioni, pena l'applicazione di sanzioni.

a) i dati trattati devono risiedere solo sulle infrastrutture informatiche e quindi non è consentito scaricare i dati/file/archivi sui dispositivi personali

b) i dati personali degli interessati non devono essere trattati per scopi differenti da quelli per cui sono stati originariamente raccolti e devono essere utilizzati solo per il tempo necessario

c) deve essere assolutamente evitata la disseminazione indistinta (ad esempio su più dispositivi) dei dati personali oggetto di trattamento tramite BYOD

d) l'accesso ai dispositivi deve essere regolamentato da apposite credenziali (es: password o PIN)

e) qualora il dispositivo personale che contiene dati del Titolare del trattamento, fosse perso, smarrito, rubato, fosse oggetto di un accesso improprio o comunque ci sono elementi per immaginare/sospettare che i dati contenuti possano essere, sia pure temporaneamente, resi accessibili a terze parti, l'incaricato deve informare immediatamente il Titolare del trattamento affinché possa essere valutata la problematica e prese, se del caso le opportune misure. La comunicazione deve essere immediata e non possono esser accettati ritardi

f) nel caso in cui il dispositivo mobile del lavoratore sia venduto, ceduto, trasferito, il contenuto deve essere cancellato/anonimizzato in modo irreversibile.

Per ogni azione di cui ai punti d), e), f) il supporto tecnico comunale è disponibile a riguardo.

e) Trattamenti senza strumenti elettronici

Per quanto riguarda la eventuale documentazione cartacea, compresi i supporti non informatici contenenti la riproduzione di informazioni relative al trattamento di dati personali, gli atti e i documenti contenenti i dati devono essere conservati, dalle persone autorizzare al trattamento dei dati personali, per la durata del trattamento e successivamente riposti in archivi ad accesso controllato, al fine di escludere l'accesso, agli stessi, da parte di persone non incaricate al trattamento o, in mancanza chiudere a chiave l'ufficio nel quale si effettua il trattamento se gli archivi sono in esso contenuti.

Nel caso di trattamento di dati sensibili, di dati di minori o di dati giudiziari, gli atti e i documenti, contenenti i dati affidati alle persone autorizzate al trattamento, devono essere conservati in contenitori muniti di serratura, al fine di escludere l'acquisizione, degli stessi, da parte di persone non autorizzate del trattamento.

La cancellazione dei dati contenuti negli archivi cartacei deve avvenire secondo i tempi/criteri contenuti nel "Registro dei Trattamenti" e previa autorizzazione de Titolare del trattamento. Potranno essere richieste la verbalizzazione di tale atto. Quando è necessario distruggere i documenti contenenti dati personali, utilizzare gli appositi apparecchi "distruggi documenti"; in assenza di tali strumenti, i documenti devono essere sminuzzati in modo da non essere più ricomponibili;

Le persone autorizzate al trattamento sono tenute a segnalare le eventuali necessità di dotazioni e arredi, in modo da poter adempiere a quanto prescritto

L'incaricato si impegna a:

- verificare che i documenti utilizzati siano sempre sotto il suo controllo e la sua custodia per l'intero ciclo necessario allo svolgimento delle operazioni relative al trattamento dei dati, al fine di garantire che i documenti non siano visti o trattati da persone non autorizzate;
- conservare i documenti, in caso di trasferimento degli stessi, in contenitori chiusi ed anonimi;
- effettuare le copie dei dati documenti cartacei solo se strettamente necessario ed in ogni caso trattarle con la stessa cura dei documenti originali, al termine del trattamento distruggere eventuali copie non utilizzate o comunque alterarle per impedirne la consultazione;
- controllare che i documenti, composti da numerose pagine o più raccoglitori, siano sempre completi, verificando che sia il numero dei fogli sia l'integrità del contenuto è conforme a quanto era presente all'atto del prelievo dal luogo sicuro;
- identificare un luogo sicuro di custodia che dia sufficienti garanzie di protezione da accessi non autorizzati. Ove si utilizzi un contenitore, un armadio o un raccoglitore chiuso a chiave, l'incaricato deve custodire le chiavi, ed accertarsi che non esistano duplicati abusivi delle stesse;
- utilizzare buste di sicurezza con chiusura auto sigillante, per la consegna di copie di documenti, se possibile eseguire la consegna personalmente al fine di ridurre al minimo la possibilità che, soggetti terzi non autorizzati, possano prendere visione del contenuto a addirittura fotocopiarlo all'insaputa del mittente e destinatario,
- non discutere, comunicare o trattare dati personali per telefono se non si è certi che il corrispondente sia un Incaricato, il cui profilo di autorizzazione sia tale da consentire l'acquisizione e il trattamento dei dati in oggetto. Questa precauzione diventa indispensabile se l'apparecchio è utilizzato in luogo pubblico o aperto al pubblico.
- non parlare mai ad alta voce, trattando dati personali, in presenza di terzi non autorizzati che potrebbero venire a conoscenza di dati personali in modo fortuito e accidentale.
- custodire le chiavi, se si utilizza un armadio e/o un contenitore con serratura, ed accertarsi che non esistano duplicati abusivi delle stesse.

L'incaricato dichiara:

- di essere a conoscenza degli obblighi derivanti da quanto di seguito riportato e da qualsiasi altro obbligo riportato nel suo mansionario;
- di essere a conoscenza che in caso venissero riscontrate azioni illecite o il mancato rispetto delle istruzioni contenute nel presente documento, il Titolare del trattamento si riserba di provvedere ad azioni disciplinari nei suoi confronti nel caso in cui gli possono essere imputate (in maniera lampante) le predette azioni illecite.

In ordine alla durata della nomina, si fa presente che la revoca della stessa avverrà con la risoluzione del contratto posto in essere tra **il Titolare del trattamento** e **l'Incaricato.**

L'incaricato con la firma della presente lettera accetta la nomina e conferma di aver preso conoscenza del presente accordo come parte integrante del contratto di lavoro e di osservarne le disposizioni nello svolgimento del proprio lavoro.

Il Comune di Ala (TN)
il sindaco

Data, _____

Per accettazione_____