CAMERA DI COMMERCIO
INDUSTRIA ARTIGIANATO E AGRICOLTURA
BRESCIA

DISCIPLINARE PER GLI AUTORIZZATI AL TRATTAMENTO

I Soggetti autorizzati al trattamento devono operare sotto la diretta autorità delle strutture preposte dal Titolare per la gestione della protezione dei dati, nel rispetto delle istruzioni loro impartite, tali da garantire la riservatezza dei dati e la sicurezza del trattamento.

Per qualsiasi altra informazione o dubbio è sempre possibile rivolgersi al Titolare al DPO o al suo Referente interno all'Ente.

Di seguito sono delineate le modalità con cui i dati, comuni, particolari e giudiziari, devono essere trattati, in conformità al Regolamento (UE) 2016/679 ed alla normativa nazionale vigente.

Ogni Dipendente nominato "Autorizzato" risponde singolarmente di eventuali usi impropri dei dati e delle informazioni in particolare se, dal fatto, ne deriva un danno ovvero un vantaggio personale.

MODALITÀ DI TRATTAMENTO DI DATI PERSONALI:

A. DATI PERSONALI COMUNI (*ex* art. 5)

L'autorizzato opera in modo tale che i dati personali comuni oggetto di trattamento siano:

1. trattati in modo lecito, corretto e trasparente nei confronti dell'Interessato ("*liceità, correttezza e trasparenza*");
2. raccolti e registrati per scopi documentati e determinati, espliciti e legittimi, ed utilizzati in altri trattamenti correlati in modo compatibile con gli scopi per cui sono stati raccolti ("*limitazione delle finalità*");
3. esatti e, se necessario, aggiornati; devono essere, inoltre, adottate tutte le ragionevoli misure per la cancellazione o la rettifica tempestiva dei dati inesatti, rispetto alle finalità del trattamento ("*esattezza*");
4. adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati ("*minimizzazione dei dati*");

5. conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati. I dati personali possono comunque essere conservati per periodi di tempo più lungo, a condizione che siano trattati esclusivamente ad archiviazione per pubblico interesse, ricerca scientifica o storica e fini statistici ("*limitazione della conservazione*");
6. trattati in maniera da garantire un'adeguata sicurezza dei dati personali - compresa la protezione mediante misure tecniche ed organizzative adeguate – da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale ("*integrità e riservatezza*").

Ai sensi degli artt. 32 e seguenti del GDPR, le attività di trattamento devono seguire le misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare – su base permanente – riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali, in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza nel trattamento.

In attuazione delle previsioni di legge gli autorizzati devono:

1. utilizzare l'autenticazione informatica, custodendo con la massima riservatezza la credenziale di accesso (user-id) e la password; le credenziali non possono essere comunicate a terzi e non possono essere custodite in chiaro; le password devono essere cambiate almeno ogni sei mesi (tre mesi in caso di trattamenti di dati particolari e giudiziari);
2. eseguire esclusivamente i trattamenti funzionali o strumentali all'esecuzione dei compiti loro attribuiti e raccogliere e trattare i soli dati personali la cui conoscenza sia strettamente necessaria per adempiere tali compiti;
3. fornire all'interessato l'informativa di cui all'articolo art. 13 del Regolamento (UE) (2016/679) così come predisposta e resa disponibile, anche mediante affissione allo sportello;
4. comunicare a terzi i dati personali solo nei casi espressamente previsti da legge o da regolamento e non utilizzare per altri fini i dati personali di cui dovessero venire a conoscenza nell'esecuzione delle operazioni suddette e comunque mantenere la più completa riservatezza sui dati trattati e sulle tipologie di trattamento effettuate. Tali obblighi sono da considerarsi pienamente vigenti anche nel caso di cessazione del rapporto di lavoro;

5. attivare la protezione degli strumenti elettronici e dei dati, rispetto a trattamenti illeciti, ad accessi non consentiti e a determinati programmi informatici;
6. seguire le indicazioni del proprio responsabile comunicate durante le attività di formazione o nei vari disciplinari operativi;
7. seguire le procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
8. per l'accesso al Sistema Informatico della Società, attenersi alle direttive in materia di sicurezza predisposte dalla Società ed informare tempestivamente quest'ultima – per il tramite del proprio Referente di Funzione interno - in caso di incidente di sicurezza che coinvolga i dati.

Nel caso in cui il trattamento sia effettuato con supporti cartacei o richieda supporti cartacei si deve prevedere:

1. idonea custodia di atti e documenti affidati agli autorizzati per lo svolgimento dei relativi compiti e loro restituzione al termine delle operazioni affidate;
2. conservazione di determinati atti in archivi ad accesso selezionato;

Per l'idonea custodia degli uffici e degli archivi di trattamento si possono adottare le seguenti semplici precauzioni:

1. chiudere a chiave la porta dell'ufficio in assenza del personale preposto;
2. mantenere la documentazione cartacea negli armadi e chiudere a chiave gli armadi al termine della giornata di lavoro;
3. mantenere la massima riservatezza con gli estranei e prestare la massima attenzione a comportamenti di personale non addetto.

Nel valutare l'adeguato livello di sicurezza, si deve in particolar modo tener conto dei rischi presentati dal trattamento dei dati, soprattutto dalla loro distruzione, perdita, modifica, divulgazione non autorizzata o dall'accesso – in modo accidentale e/o illegale – ai dati personali trasmessi, conservati o trattati.

In caso di violazione delle normative e delle regole, l'autorizzato deve informare tempestivamente il proprio Referente di Funzione interno e seguire le eventuali indicazioni che egli darà per minimizzare le ricadute sull'Ente.

Va ricordato che ai sensi degli artt. 33 e seguenti del Regolamento, in caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'Autorità di Controllo competente, senza ingiustificato ritardo e, se possibile, entro le successive 72 ore dalla venuta a conoscenza.

Inoltre, quando la violazione dei dati personali è suscettibile di presentare un elevato rischio per i diritti e le libertà delle persone fisiche, il Titolare del Trattamento comunica la violazione all'Interessato senza ritardo ingiustificato.

B. DATI PERSONALI PARTICOLARI (*ex* art. 9 GDPR)

Il Regolamento (UE) 679/2016 sancisce il divieto di trattamento di dati "*personali che rilevino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi ad identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*".

L'Autorizzato al trattamento di dati personali particolari è tenuto ad operare nel rispetto delle seguenti modalità:

a) le operazioni di accesso e di trattamento di tali dati dovranno essere effettuate esclusivamente dalle rispettive stazioni di lavoro;

b) nel momento in cui i dati particolari sono relativi ai dipendenti della Società, e quindi legati alla gestione del Personale, ovvero ove si trattino dati storici compresi eventuali file di pertinenza dell'interessato, questi devono essere conservati in un archivio riservato dell'Ufficio Risorse Umane e Organizzazione opportunamente predisposto; tali file devono inoltre essere archiviati su supporto permanente (ad es. File Server);

c) nel caso in cui il trattamento sia effettuato con supporti cartacei o richieda supporti cartacei si deve attuare idonea custodia tramite conservazione di quei determinati documenti (o atti) contenenti dati particolari, in archivi ad accesso selezionato o chiuso o in un ufficio presidiato, o in un armadio/cassetto dotato di serratura con chiave; quest'ultima affidata in custodia all'incaricato del trattamento debitamente autorizzato;

e) la stampa dei documenti contenenti dati particolari deve essere effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato del trattamento. Detti documenti vanno eliminati, quando non sia più necessario conservarli per gli scopi per cui sono stati stampati;

f) le informazioni residue - ossia quei dati particolari ancora leggibili dopo la cessazione di un trattamento vanno distrutte o quanto meno rese illeggibili, a meno che debbano essere conservate.

Tenuto conto dei particolari limiti e garanzie che il Regolamento Ue n. 679/2016 prevede, l'Autorizzato è tenuto al compimento delle attività di trattamento nel pieno rispetto della normativa vigente e soprattutto delle peculiarità previste - ai sensi dell'art. 9 del GDPR – per i dati personali particolari.

C. DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI (*ex* art. 10 GDPR)

Con specifico riguardo al trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, ai sensi dell'art. 10 del Regolamento UE n. 679/2016, esso "*deve avvenire soltanto sotto il controllo dell'Autorità Pubblica o se il trattamento è autorizzato dal diritto dell'Unione o dagli Stati*

membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'Autorità pubblica".

Per la natura dei dati trattati di tipo giudiziario, l'attenzione da prestare sul trattamento dei dati stessi in relazione al tema Privacy, normato dal Regolamento (UE) 2016/679, deve essere molto puntuale, mantenendo la massima riservatezza nello svolgimento delle attività e nella custodia di tali informazioni, siano esse in forma elettronica siano in forma cartacea.

Data la particolarità dei dati trattati si precisa:

- il divieto di apertura di buste contenenti atti giudiziari, se non in ottemperanza alle disposizioni ricevute e per lo svolgimento del proprio compito lavorativo;
- l'obbligo di segretezza;
- il divieto di stampare documenti contenenti dati giudiziari, salvo particolari esigenze d'ufficio, in tal caso la stampa deve essere effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato del trattamento;
- la loro eliminazione, quando non sia più necessario conservarli per gli scopi per cui sono stati stampati;
- il cambio delle password di accesso ai sistemi ogni tre mesi.

Ogni accesso e/o comunicazione e/o diffusione di dati verso soggetti esterni dovrà essere autorizzato preventivamente dal proprio Referente di Funzione interno.

IL SEGRETARIO GENERALE

(dr Massimo Ziletti)

Firma digitale ai sensi dell'art. 24 del d.lgs. 7 marzo 2005 n. 82

"Codice dell'Amministrazione digitale"