

Disposizioni Incaricati AMT

ALLEGATO ALLA LETTERA DI NOMINA AD INCARICATO DEL TRATTAMENTO

Principali disposizioni al dipendente incaricato del trattamento di dati personali ai sensi del decreto legislativo 196/2003 “codice in materia di protezione dei dati personali”.

In riferimento alla nomina conferitaLe quale “Incaricato del trattamento di dati personali”, La invitiamo a osservare scrupolosamente le seguenti disposizioni.

I dati personali da Lei trattati dovranno riferirsi esclusivamente agli ambiti ed alle banche dati cui Lei è autorizzato/a a trattare e ad accedere e solo per le finalità e le tipologie determinate, esplicite e legittime, indicate dal Responsabile nella lettera di conferimento della nomina ad Incaricato.

I dati personali dovranno essere trattati in modo lecito e secondo correttezza.

L'utilizzazione di dati raccolti e registrati in un trattamento potranno essere utilizzati in altre operazioni di trattamento autorizzato solo in termini compatibili con tali scopi.

I dati personali dovranno essere esatti e, se necessario, dovranno essere aggiornati dagli uffici competenti ciascuno per il proprio ambito di responsabilità.

I dati personali dovranno essere pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati.

I dati personali dovranno essere conservati, rispettando le misure di sicurezza predisposte, o che verranno ulteriormente introdotte, dal Titolare/Responsabile che sono previste in conformità alla Normativa Privacy ed in una forma che consenta l'identificazione dell'interessato (inteso come la persona fisica o giuridica i cui dati sono trattati; di seguito, l' "Interessato") per un periodo di tempo non superiore a quello necessario agli scopi per cui i dati sono stati raccolti o successivamente trattati.

Qualora sia necessario distruggere i documenti contenenti dati personali questi devono essere distrutti utilizzando gli appositi apparecchi “distruggi documenti” o, in caso di loro assenza, i documenti devono essere sminuzzati in modo da non essere più componibili; i supporti magnetici od ottici contenenti dati personali devono essere cancellati prima di essere riutilizzati; se ciò non è possibile essi devono essere distrutti.

Lei dovrà partecipare alle attività di formazione privacy organizzate dal Titolare/Responsabile.

Qualora uno o più Interessati denunzino situazioni o fatti rilevanti di particolare gravità, dovrà informarne tempestivamente per iscritto il Responsabile ed adottare tutte le misure precauzionali e/o riparatorie necessarie.

La comunicazione o la diffusione dei dati personali a terzi, dipendenti o meno del Titolare, anche all'estero ed anche al di fuori dell'Unione Europea, può essere fatta esclusivamente ai soggetti autorizzati a ricevere legittimamente tali dati, per le finalità per le quali i dati sono stati raccolti e comunque nel pieno rispetto delle istruzioni ricevute dal Titolare/Responsabile, delle Policy aziendali ed in conformità alla Normativa Privacy.

E' sempre vietato, salvo autorizzazione scritta del Titolare/Responsabile:

- estrarre copia di banche dati o di singoli dati al di fuori dell'incarico ricevuto ovvero creare nuove ed autonome banche dati;
- raccogliere ed in qualsiasi modo trattare dati personali al di fuori dell'incarico ricevuto.

Nell'ambito dei compiti cui è preposto/a, Lei dovrà collaborare con il Responsabile per garantire i diritti degli Interessati in conformità a quanto disposto dall'art. 7 del Codice Privacy. In particolare, dovrà collaborare per:

- confermare l'esistenza o meno di dati personali che riguardano l'Interessato, anche se non ancora registrati, ed effettuare la loro comunicazione in forma intelligibile;
- fornire l'indicazione dell'origine dei dati personali;
- fornire l'indicazione delle finalità e delle modalità del trattamento;
- fornire l'indicazione della logica applicata (in caso di trattamento effettuato con l'ausilio degli strumenti elettronici);
- fornire l'indicazione dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentanti designati nel territorio dello Stato, di responsabili o incaricati;
- fornire l'aggiornamento, la rettificazione ovvero, quando l'Interessato vi ha interesse, l'integrazione dei dati;
- effettuare la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
- fornire l'attestazione che le operazioni di cui ai precedenti due punti sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato;
- accogliere l'opposizione dell'interessato nei casi di cui al comma. 4 del Codice Privacy;
- rispettare ogni altra prescrizione prevista dagli articoli 7 e 8 del Codice Privacy.)

Qualora Lei dovesse allontanarsi anche temporaneamente dalla Sua postazione dovrà verificare che non vi sia possibilità da parte di terzi non autorizzati di accedere in qualsiasi modo ai dati personali per i quali è in

corso un qualsiasi tipo di trattamento; in caso di trattamento dati tramite strumenti elettronici, dovrà sospendere la sessione di lavoro.

Quando lascia la Sua postazione, ad esempio al termine dell'orario di lavoro, Lei dovrà identificare un luogo sicuro di custodia degli atti e dei documenti in Suo possesso, in modo da evitare accessi non autorizzati ai dati (ad esempio un armadio, un cassetto, un classificatore chiuso a chiave).

Qualora sia necessaria l'asportazione di tali dati al fine di espletare le mansioni affidate, Lei dovrà farlo limitatamente ai documenti strettamente necessari e per il tempo minimo a tal fine necessario.

Lei dovrà limitare al minimo il numero di fotocopie eventualmente effettuate e trattare queste ultime con le medesime cautele utilizzate per i documenti originali.

In caso di trattamento di dati con strumenti elettronici, Le verranno assegnate credenziali di autenticazione che consentano il superamento di una procedura di autenticazione e l'accesso al sistema di autorizzazione del Titolare.

Le credenziali di autenticazione consistono in un codice per la Sua identificazione associato a una parola chiave riservata conosciuta solamente da Lei.

Lei dovrà modificare la parola chiave immediatamente, al primo utilizzo, e successivamente almeno ogni sei mesi per i dati personali comuni e tre mesi per i dati sensibili. A tale proposito Le verrà inviato un messaggio che La avvertirà della scadenza e Le richiederà di inserire una nuova parola chiave, che dovrà essere mantenuta strettamente riservata. La parola chiave dovrà essere composta da almeno otto caratteri. Lei dovrà adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale di autenticazione (vale a dire la parola chiave); la parola chiave che Lei deciderà di usare non deve contenere riferimenti agevolmente riconducibili a Lei. In caso di dubbi, anche minimi, sulla possibilità che la segretezza della Sua parola chiave sia stata compromessa, Lei dovrà immediatamente procedere alla sostituzione della parola chiave. Lei dovrà attenersi alle procedure aziendali e garantire nell'ambito del sistema informativo del Titolare un trattamento lecito, corretto, sicuro e conforme alla Normativa Privacy, ad esempio le istruzioni per la diligente custodia e l'uso dei dispositivi in Suo possesso, custodia ed uso esclusivo e dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti, per il salvataggio dei dati, anche mediante apposite procedure interne che Le saranno comunicate e rese disponibili.

Al fine di assicurare la disponibilità di dati o strumenti elettronici accessibili solo mediante uso delle proprie credenziali di autenticazione - ad esempio file criptati, password di amministratore sistema (qualora sia unico) etc.. - in caso di Sua prolungata assenza ovvero Suo impedimento che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, gli incaricati dei sistemi informativi provvederanno a creare, a seguito di apposita autorizzazione, un nuovo utente con opportuno profilo.

Lei dovrà denunciare immediatamente al soggetto che sovrintende quale Responsabile del trattamento la Direzione/Area alla quale Lei appartiene o che è di Sua competenza disfunzioni del sistema informatico ovvero episodi che possano in qualsiasi modo determinare pericolo nel trattamento o nella sicurezza dei dati.

Se Lei ha bisogno di accedere ai locali aziendali dopo l'orario di chiusura, dovrà informarne il suo Responsabile affinché questi verifichi le ragioni della richiesta ed in caso di necessità provveda per la Sua autorizzazione, illustrandoLe, anche in collaborazione con il Responsabile del sistema informativo aziendale, le procedure adottate per la Sua identificazione e registrazione. Il controllo agli accessi potrà essere effettuato mediante strumenti elettronici e non elettronici.

Per quanto riguarda il trattamento di dati personali comunicati per telefono, si raccomanda vivamente di non parlare mai ad alta voce per telefono, soprattutto quando si usano apparecchi cellulari, sia all'esterno sia all'interno dei locali aziendali e si è in presenza di terzi non autorizzati, per evitare che dati personali possano venire a conoscenza di terzi non autorizzati, anche accidentalmente. Le stesse precauzioni devono essere adottate in caso di uso di telefoni pubblici ovvero situati all'interno dei locali aziendali.

La invitiamo infine ad informare prontamente e previamente per iscritto il Titolare/Responsabile (i) qualora si verifichi la necessità di porre in essere operazioni di trattamento di dati personali per finalità o con modalità diverse da quelle risultanti dalle istruzioni da Lei ricevute; (ii) in caso di qualsiasi richiesta, ordine od attività di controllo da parte del Garante per la protezione dei dati personali o dell'autorità giudiziaria, ovvero qualsiasi richiesta od istanza di qualsiasi genere e contenuto da parte di Interessati; e (iii) in caso si realizzi qualsiasi circostanza che esuli dalle istruzioni che Le sono state impartite, ad esempio episodi o fatti rilevanti occorsi nel trattamento dei dati cui Lei è preposto quali ad esempio eventuali accessi non autorizzati ai dati, situazioni anomale, eventuali irregolarità.

Qualora le Sue mansioni lavorative prevedono la gestione di sistemi informativi dovrà inoltre attenersi a quanto indicato di seguito:

- Su richiesta del Titolare e/o degli altri responsabili nominati dal Titolare, dovrà verificare l'ambito di trattamento consentito all'utente, compresi eventuali profili di autorizzazione e provvedere all'attribuzione di un codice identificativo univoco e di una parola chiave (*password*).
- Al momento dell'attribuzione delle credenziali di autenticazione, dovrà fornire all'utente una parola chiave che dovrà essere modificata dall'utente al primo utilizzo come descritto in precedenza. Ad ogni utente potranno essere assegnate ovvero associate individualmente una o più credenziali per l'autenticazione; il codice per l'identificazione assegnato ad un utente non potrà essere assegnato ad altri utenti, neppure in tempi diversi.
- La parola chiave dovrà essere composta da almeno otto caratteri. Le credenziali di autenticazione non utilizzate da almeno sei mesi devono essere disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica. Le credenziali di autenticazione dovranno essere disattivate anche in caso di perdita della qualità che consente all'utente l'accesso ai dati personali.

- Al fine di assicurare la disponibilità di dati o strumenti elettronici accessibili solo mediante uso delle credenziali di autenticazione in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, dovrà attenersi alle indicazioni riportate in precedenza.
- Comunicare al Titolare/Responsabile per la gestione del sistema informativo nominato dal Titolare eventuali accessi non autorizzati ai dati personali, situazioni anomale ed eventuali altre irregolarità delle quali abbia conoscenza.

Maggiori dettagli e approfondimenti riguardanti le istruzioni operative sono contenuti nel sito intranet aziendale.

Nell'ambito dei compiti cui Lei è preposto/a, dovrà avere cura a che i dati sensibili ed i dati giudiziari, o i dati che, per qualsiasi ragione, siano stati indicati dal Titolare/Responsabile come meritevoli di particolare attenzione al momento dell'affidamento a Lei, o che siano anche successivamente indicati come tali, siano raccolti e trattati nel pieno rispetto delle particolari garanzie imposte dalla Normativa Privacy e dalle istruzioni fornite dal Titolare/Responsabile per le suddette categorie di dati e che sono meglio dettagliate nel sito intranet aziendale.