ISTRUZIONE ALLE PERSONE AUTORIZZATE AL TRATTAMENTO DEI DATI PERSONALI

Il Codice sulla privacy (art. 30) imponeva originariamente all'azienda titolare del trattamento di designare gli "incaricati del trattamento" e di fornire a tutte queste persone istruzioni scritte. La designazione e la definizione delle istruzioni veniva compiuta dal titolare del trattamento o dal/i responsabile/i se nominato/i.

Il Regolamento UE n. 679/2016 non delinea invece in modo esplicito la figura di "incaricato", sebbene da diverse disposizioni (vedi l'art. 4 n. 10 e 28, 3°paragrafo, lettera b) emerga la figura delle "persone autorizzate al trattamento", confermando in sostanza la figura ed il ruolo degli incaricati. In base all'articolo 29 del regolamento (vedi anche l'art. 32, 4°paragrafo) tali persone debbono ricevere istruzioni da parte del titolare; l'art. 4 n. 10 precisa anche che operano sotto l'autorità diretta del titolare o del responsabile.

E' quindi opportuno che l'azienda verifichi, ed eventualmente aggiorni con regolare periodicità, l'elenco delle persone autorizzate al trattamento di dati personali, oltre che dei relativi ambiti di trattamento consentiti (come, peraltro, già prevedeva il previgente disciplinare tecnico allegato al Codice privacy). Pur non venendo previsto l'onere di formalizzare per iscritto la nomina di tali persone e le conseguenti istruzioni, l'utilizzo di una nomina di designazione scritta appare senz'altro la preferibile, rimanendo infatti la finalità delle istruzioni scritte quella di individuare gli specifici trattamenti che la persona autorizzata può legittimamente compiere conformemente alle proprie mansioni aziendali.

Le istruzioni di cui sopra devono inoltre contenere l'individuazione delle banche dati cui la persona autorizzata può accedere, la definizione delle finalità per le quali si effettuano i trattamenti, l'eventuale ambito di comunicazione e/o diffusione all'esterno.

Infine, in ragione degli specifici obblighi in materia di sicurezza imposti all'azienda dal Regolamento (artt. 24 e 32), è necessario dettare anche prescrizioni puntuali sulle misure di sicurezza adottate a tutela dei dati: queste misure dovranno essere osservate da ogni singola persona autorizzata, anche al fine di garantire la necessaria riservatezza (art. 28, 3°paragrafo lettera b). Dal punto di vista gestionale delle misure di sicurezza per i trattamenti informatici, le diverse mansioni (e, di conseguenza, le banche dati con le relative diverse finalità di trattamento) si concretizzano, opportunamente, in un sistema di autenticazione all'accesso del sistema informatico che prevede diversi profili di autorizzazione. Si ricorda che viene consigliata la predisposizione di un apposito e specifico regolamento o policy sull'uso degli strumenti di lavoro da rivolgere, anche ai fini di informazione per la privacy a tutto il personale.

Modello di designazione del personale addetto al trattamento di dati personali e relative istruzioni

Si ritiene che le istruzioni possono essere nominative od anche per gruppi omogenei di lavoro o per funzioni aziendali (come già prevedeva il Codice privacy ed il disciplinare tecnico); in caso di cambiamento di mansioni che comportino la variazione delle finalità del trattamento da svolgere o il mutamento dei data base accessibili, è necessario modificare le istruzioni scritte già fornite. Possono essere autorizzate al trattamento dei dati personali solo le persone fisiche.

Egr. Signor/Signora

Il Regolamento UE 2016/679 (regolamento generale sulla protezione dei dati) ed il Codice sulla privacy (D.lgs. 30 giugno 2003, n.196, per come modificato dal D.lgs. 10 agosto 2018, n.101) sulla tutela della riservatezza nel trattamento di dati personali hanno introdotto rilevanti obblighi a carico dell'impresa, obblighi la cui inosservanza è sanzionata anche penalmente ed espone a responsabilità civili.

Queste norme hanno la finalità di garantire che il trattamento di dati personali si svolga nel pieno rispetto dei diritti dell'interessato, ovvero la persona fisica cui i dati si riferiscono.

In particolare, il Regolamento generale prescrive (art. 29) che vengano impartite da parte del titolare dell'impresa specifiche istruzioni alle "persone autorizzate al trattamento" e, cioè, a coloro che, nell'ambito dell'organizzazione stessa ed in relazione alle mansioni affidate, trattano dati personali sia mediante sistemi informatici che mediante documenti cartacei.

Pertanto, nell'ambito delle mansioni a Lei assegnate, viene designato "persona autorizzate al trattamento" e le vengono impartite le seguenti istruzioni atte a garantire un trattamento lecito, corretto e sicuro dei dati.

Accesso a banche dati aziendali

Le banche dati cui è autorizzato ad accedere per effettuare i trattamenti (sia informatici che cartacei), sempre strettamente pertinenti alle mansioni svolte e per le finalità previste dall'azienda, rispettando i principi fondamentali sanciti dall'art. 5 del Regolamento generale sulla protezione dei dati e garantendo la riservatezza degli stessi dati, sono le seguenti: banca dati marketing, banca dati clienti, banca dati controllo qualità, banca dati personale.

Creazione nuove banche dati. Gestione programmi

Senza preventiva autorizzazione del Titolare non è permesso realizzare nuove ed autonome banche dati, con finalità diverse da quelle già previste.

Trattamento dei dati personali

Il trattamento dei dati personali deve essere effettuato esclusivamente in conformità alle finalità previste e dichiarate dall'azienda e, pertanto, in conformità alle informazioni che l'azienda ha comunicato agli interessati. L'eventuale raccolta di dati dovrà avvenire nel rispetto delle procedure e dei modelli di informativa e/o consenso elaborati dall'azienda.

Le finalità per le quali è autorizzato a trattare i dati personali nell'ambito delle mansioni svolte sono le seguenti: Gestione amministrativa dell'azienda, compresa la parte di fatturazione attiva e passiva.
La persona autorizzata deve prestare particolare attenzione all'esattezza dei dati trattati e provvedere, inoltre, all'aggiornamento degli stessi.

Comunicazione e diffusione dei dati

In relazione alle banche dati di cui è autorizzato il trattamento nello svolgimento delle mansioni affidate, è autorizzata la comunicazione dei dati stessi esclusivamente ai seguenti soggetti esterni indicati dall'azienda: si cita istituti di credito per i pagamenti, società di recupero crediti per attività di recupero, società di assicurazione del credito, legali per recupero crediti.

Ogni ipotesi diversa di comunicazione o, addirittura, di diffusione dei dati dovrà essere preventivamente autorizzata di volta in volta dall'impresa.

Misure di sicurezza

Ogni persona autorizzata è tenuta ad osservare tutte le misure di protezione e sicurezza atte a evitare rischi di distruzione, perdita, accesso non autorizzato, trattamento non consentito, già predisposte dall'impresa, nonché quelle che in futuro verranno comunicate.

Sistemi informatici *(le indicazioni si riferiscono alle originarie misure minime obbligatorie elencate nel disciplinare tecnico allegato al Codice. In base al nuovo principio di "responsabilizzazione" (art. 5, 2° paragrafo), è onere dell'azienda, titolare del trattamento organizzare e documentare un sistema di misure di sicurezza atto a garantire la integrità e riservatezza dei dati personali trattati, art. 5, 1° paragrafo, lettera f).*

Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale del Servizio ICT.
Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, si procederà in tal senso d'intesa con il personale del Servizio ICT.
Soggetto preposto alla custodia delle credenziali di autenticazione è il personale del Servizio ICT di PR Ecology s.r.l..

Si ricorda che l'azienda titolare del trattamento, nei casi in cui è indispensabile ed indifferibile accedere ai dati trattati dalla persona autorizzata ed agli strumenti informatici in dotazione alla stessa sia per le esigenze produttive aziendali sia per la sicurezza ed operatività dello stesso sistema informatico (ad esempio nei casi di prolungata assenza od impedimento della persona), potrà accedere mediante intervento del custode delle credenziali nominato dall'azienda stessa.

La persona autorizzata non può installare ed utilizzare programmi per elaboratore non autorizzati dall' azienda né privi di licenza che legittimino l'uso. (2)

Gli strumenti informatici e telematici messi a sua disposizione (computer, software, navigazione su internet, e- mail) costituiscono degli strumenti di lavoro da utilizzare esclusivamente per l'esecuzione delle mansioni affidate (2).

Trattamenti cartacei

In base al principio di stretta pertinenza dei trattamenti rispetto alle mansioni svolte, potrà accedere agli archivi relativi alle banche dati di tipo cartaceo ubicate presso Via Antonini 14 a Fontanafredda (PN).

La persona autorizzata, nel trattare documenti contenenti dati particolari o giudiziari è tenuta a custodirli fino alla restituzione in modo da evitare l'accesso agli stessi dati a persone prive di autorizzazione. La persona autorizzata deve, inoltre, custodire gli archivi contenenti documenti con dati sensibili e giudiziari, ed evitare che personale non autorizzato vi acceda. L'accesso fuori dall'orario di lavoro impone la registrazione e l'identificazione delle persone ammesse ai locali.

I documenti (o copia degli stessi) non possono, senza specifica autorizzazione, essere portati fuori dai luoghi di lavoro, salvo i casi di comunicazione dei dati a terzi preventivamente autorizzati in via generale dall'azienda.

Violazione dei dati personali (Data breach)

In caso di incidenti che possono determinare una violazione di dati personali ("Data Breach"), dovrà immediatamente comunicare la possibile violazione al Servizio ICT, al fine di permettere all'azienda di attivare la procedura di verifica degli eventi e di adempiere, se del caso, agli obblighi di notifica e di comunicazione previsti dagli articoli 33 e 34 del Regolamento UE 2016/679 a carico del titolare del trattamento. Si tenga a mente che per "Data Breach" ai sensi del citato Regolamento UE, si intende qualsiasi violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso abusivo (cioè non autorizzato) ai dati personali gestiti dall'azienda, siano essi archiviati, trasmessi o comunque in altro modo trattati.

data 14/01/2025

---

(1) In molti sistemi la comunicazione di variazione può essere "generata" dallo stesso sistema informatico all'atto della modifica, con invio di e-mail automatica al custode; molti sistemi permettono di "temporizzare" la validità delle password e, quindi, di bloccare l'accesso al personale computer e/o al sistema, qualora non venga autonomamente variata dalla persona autorizzata entro i termini massimi: in questi casi, vanno adattate le istruzioni contenute nel presente regolamento, eliminando, tra l'altro l'onere di comunicazione della variazione al custode delle credenziali.

(2) Si possono eventualmente aggiungere prescrizioni in ordine alle questioni della tutela del diritto d'autore sul software (possesso di regolari licenze su tutto il software installato e divieto di installazione di software non coperto da licenza o, comunque, non preventivamente autorizzato dall'azienda), sulla tutela del know-how aziendale (individuazione di aree e tipologie di documenti di maggior rilievo per l'azienda da contraddistinguere quali documenti o aree in cui si gestisce know-how riservato dell'azienda) e sull'uso quali strumenti di lavoro della posta elettronica e della navigazione di internet anche ai fini della tutela dai virus.

Queste indicazioni non concernono in senso stretto la tutela della privacy, ma sono consigliabili per una corretta gestione dei sistemi informatici e delle informazioni in azienda: questo insieme di prescrizioni potrebbero essere oggetto di un separato "*Codice di comportamento o regolamento aziendale*" (riportato tra i modelli) adottato dall'azienda e comunicato ai dipendenti.