ISTRUZIONI INCARICATI

Sommario

Introduzione

Il presente documento costituisce un manuale con istruzioni operative per il corretto utilizzo dei sistemi informatici presenti nell'azienda nell'ambito delle attività di trattamento dei dati personali o particolari. Lo scopo è quello di ridurre e contenere i rischi di danneggiamento o dispersione dei dati trattati dall'azienda, a causa di un uso non corretto o illecito dei sistemi informatici da parte del personale addetto al trattamento.

I dati personali devono essere trattati:

a. in osservanza dei criteri di riservatezza;
b. in modo lecito e secondo correttezza;
c. per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati;
d. nel pieno rispetto delle misure minime di sicurezza, custodendo e controllando i dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Altri riferimenti

In relazione all'organizzazione ed alla pianificazione delle attività di trattamento dei dati, possono essere consultati anche i seguenti documenti:

- Codice in materia di protezione dei dati personali, decreto legislativo 30 giugno 2003, n.196.
- Regolamento Europeo 679/016

Organizzazione del documento

Il documento è suddiviso in quattro parti:

1. **Sicurezza fisica**: norme per la custodia e la protezione dei dati e degli strumenti utilizzati per effettuarne il trattamento;
2. **Sicurezza logica**: contromisure minime per garantire la protezione e la riservatezza dell'accesso ai dati ed agli strumenti utilizzati per il loro trattamento;
3. **Istruzioni agli incaricati del trattamento dei dati**: indicazioni utili per la corretta gestione e custodia degli account di accesso ai sistemi informatici utilizzati per il trattamento dei dati;
4. **Sicurezza del software e dell'hardware**: norme per la corretta gestione degli apparati informatici e del software installato su di essi;
5. **Sanzioni per inosservanza delle norme**: sanzioni a carico dell'autorizzato in caso di violazioni delle istruzioni operative.

Sicurezza fisica

I dati personali sia in forma cartacea che elettronica devono essere protetti in modo da impedire l'accesso a persone non autorizzate con l'obiettivo di non diffondere dati di natura riservata e al tempo stesso di preservarne l'integrità.

La sicurezza fisica riguarda quelle misure adottate al fine di impedire l'accesso di persone non autorizzate ai dati (qualora siano archiviati su supporti cartacei) o ai dispositivi informatici utilizzati per il trattamento, l'elaborazione automatica e l'archiviazione dei dati stessi. Le misure di sicurezza fisica riguardano anche le procedure organizzative e gli strumenti adottati al fine di garantire l'integrità e la conservazione dei dati a fronte di eventi straordinari dovuti a cause naturali o provocati al fine di danneggiare l'azienda.

Le misure da attuare, se non già operative, richiedono l'ubicazione dei dati (cartacei o su supporti informatici) in locali protetti da serrature e che richiedono un accesso controllato. I documenti cartacei devono essere archiviati in mobili protetti da serrature e deve essere tracciato l'iter di una pratica secondo procedure definite. La verifica della corretta adozione di quanto previsto dalle procedure da parte degli incaricati.
Nel caso di trattamento informatico sono in vigore procedure di controllo d'acceso alla sala server e ai locali dove sono ubicati gli altri sistemi informatici utilizzati per il trattamento di dati personali. Gli incaricati accedono ai dati personali secondo procedure definite ed evitano comportamenti che possano pregiudicare la riservatezza dei dati. Per esigenze specifiche chiedono indicazioni e direttive al titolare del trattamento dati di loro pertinenza.

Procedure UFFICI DI SEGRETERIA

1. Gli addetti conservano in cartelle chiusa i documenti cartacei in elaborazione.
2. Durante le pause o in caso di allontanamento dalla propria postazione i materiali cartacei vanno riposti nelle cartelle chiuse; nessun documento contenente dati personali può essere visibile.
3. L'eventuale passaggio di materiale cartaceo da un settore ad un altro per la prosecuzione o il completamento di una procedura deve avvenire attraverso la consegna di cartelle chiuse; eventuali comunicazioni orali vanno effettuate con tono di voce contenuto avvicinandosi al destinatario.
4. A fine lavoro le cartelle contenenti i documenti cartacei in elaborazione vanno depositati armadi/cassetti chiusi.
5. Concluso il servizio, le porte di accesso agli uffici devono essere chiuse a chiave. Le chiavi sono conservate in portineria.

Procedure DOCENTI

1. Ad ogni docente viene assegnato un armadietto per il deposito dei documenti contenenti dati degli alunni (prove scritte, temi, elaborati,…).
2. Gli elaborati degli alunni non devono rimanere incustoditi sulle cattedre o sui tavoli di lavoro.

Sicurezza logica

La sicurezza logica riguarda l'accesso ai dati personali trattati attraverso procedure informatiche e viene realizzata assicurando che gli accessi ai sistemi informativi avvengano secondo modalità predefinite, tali da garantire un elevato livello di robustezza ed affidabilità. In particolare, le misure di sicurezza logica mirano ad identificare gli utenti che accedono ai sistemi informatici adibiti al trattamento di dati, in modo tale da assicurare che soltanto gli incaricati autorizzati a compiere un determinato trattamento possano accedere ai dati di propria competenza. Tale identificazione avviene utilizzando un codice identificativo personale (username) associato univocamente ad ogni singolo incaricato ed una parola chiave (password).

Tutti gli incaricati devono rispettare le seguenti disposizioni:

1. L'autorizzato a cui è stato assegnato un account di identificazione (una coppia formata da uno username e da una password) per l'accesso alla rete informatica e/o all'utilizzo di applicazioni informatiche centralizzate o locali, è responsabile di tutto quanto accade a seguito di operazioni abilitate dal proprio codice identificativo personale.
2. L'autorizzato cambierà la password al primo accesso ed almeno ogni 6 mesi (3 mesi nel caso sia autorizzato al trattamento di dati sensibili).
3. L'autorizzato utilizzerà il codice identificativo personale ed una parola chiave che dovrà essere da Lei modificata almeno ogni tre mesi, attenendosi alle istruzioni tecniche impartite. La parola chiave è strettamente personale, riservata e deve essere mantenuta segreta. Ogni qualvolta la parola chiave verrà modificata dovrà immediatamente comunicarlo in busta chiusa all'autorizzato nominato custode delle parole chiave;
4. L'autorizzato gestirà le proprie password secondo le disposizioni riportate all'interno del presente regolamento.
5. L'autorizzato custodisce le password in modo riservato e non le comunica a nessun altro.
6. L'autorizzato eserciterà tutte le azioni necessarie per evitare che altre persone abbiano accesso alla sua stazione di lavoro. A tal fine quando si allontana dalla propria stazione esce dal sistema (logoff) o blocca il personal computer con la password di uno screen saver.
7. L'autorizzato utilizzerà password forti (ad es. combinazione di lettere maiuscole, minuscole, numeri e caratteri speciali, acronimi di frasi semplici, utilizzare un generatore di password, evitare password che contengano riferimenti personali, non ripetere la stessa password su diversi applicativi o siti).
8. L'autorizzato eviterà di creare nuove banche dati senza espressa autorizzazione del titolare;
9. L'autorizzato custodirà i supporti contenenti dati con particolare cura ed attenzione; i supporti non più utilizzati, prima della loro distruzione, dovranno essere cancellati in maniera irreversibile, in modo che le informazioni contenute non siano in alcun modo recuperabili. In caso di riutilizzo dei supporti, i dati dovranno prima essere cancellati in maniera irreversibile (attraverso adeguata formattazione);
10. L'autorizzato manterrà assoluto riserbo sui dati e informazioni di cui viene a conoscenza nell'esercizio delle Sue funzioni, avendo cura di rimuovere a fine lavoro i documenti dalla scrivania/piano di lavoro;
11. L'autorizzato utilizzerà i software e gli strumenti aziendali esclusivamente per i fini strettamente necessari allo svolgimento del proprio lavoro. Gli accessi ad internet e le caselle di posta elettronica aziendale non possono essere utilizzati per uso personale. Nessun software può essere installato sul proprio personal computer senza preventiva autorizzazione del titolare;
12. L'autorizzato eviterà di portare fuori dall'azienda supporti informatici o cartacei contenenti dati personali, salvo casi eccezionali che dovranno essere preventivamente autorizzati dal titolare;
13. L'autorizzato eviterà di collegare agli strumenti aziendali supporti di Sua proprietà (es. tablet, smartphone, dischi esterni, chiavette, ecc.).

Oltre a queste misure, che ogni singolo addetto al trattamento è tenuto ad adottare, l'azienda ha messo in atto e si impegna a gestire contromisure di sicurezza logica, quali firewall ed altri sistemi di filtraggio del traffico di rete, per impedire l'accesso al sistema informativo da parte di utenti non autorizzati.

Istruzioni agli incaricati del trattamento dei dati

Avuto riguardo alle attività svolte nell'ambito della Struttura di appartenenza, l'autorizzato dovrà effettuare trattamenti di dati personali di competenza attenendosi scrupolosamente alle seguenti istruzioni ed ad ogni ulteriore indicazione, anche verbale, che potrà essere fornita dal "Titolare del trattamento".

Le misure di sicurezza sono obbligatorie e sono distinte in funzione delle seguenti modalità di trattamento dei dati:

1. senza l'ausilio di strumenti elettronici (es. dati in archivi cartacei o su supportomagnetico/ottico);
2. con strumenti elettronici (PC, elaboratori, tablet, smartphone, ecc.).

Trattamenti senza l'ausilio di strumenti elettronici

I dati personali conservati su supporti informatici sono sottoposti alle stesse misure di protezione relative ai supporti cartacei. Nel caso in cui esistano copie o riproduzioni di documenti che contengono dati personali, esse devono essere protette con le stesse misure di sicurezza applicate agli originali.

Custodia

- I documenti contenenti dati personali devono essere custoditi in modo da non essere accessibili a persone non incaricate del trattamento (es. armadi o cassetti chiusi a chiave).
- I documenti contenenti dati personali prelevati dagli archivi per l'attività quotidiana, devono esservi riposti a fine giornata.
- I documenti contenenti dati personali non devono rimanere incustoditi su scrivanie o tavoli di lavoro.

Comunicazione

L'utilizzo dei dati personali deve avvenire in base al principio del "need to know" e cioè essi non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative (anche se queste persone sono a loro volta incaricate del trattamento). I dati non devono essere comunicati all'esterno della struttura e comunque a soggetti terzi se non previa autorizzazione e verifica dell'identità del soggetto a cui saranno comunicati.

Distruzione

- Qualora sia necessario distruggere i documenti contenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere sminuzzati in modo da non essere più ricomponibili.

- I supporti contenenti dati personali devono essere cancellati prima di essere riutilizzati. Se ciò non è possibile, essi devono essere distrutti.

Istruzioni per il trattamento di dati sensibili e/o giudiziari

- I documenti o i supporti che contengono dati di categorie particolari (sensibili o giudiziari) devono essere controllati e custoditi dagli autorizzati i quali devono impedire l'accesso a persone prive di autorizzazione. La consultazione di documenti per l'inserimento in procedure informatiche deve avvenire per il tempo strettamente necessario alla digitazione stessa e, subito dopo, i documenti devono essere archiviati in base alle presenti istruzioni.

- L'archiviazione dei documenti cartacei contenenti dati di categorie particolari (sensibili o giudiziari) deve avvenire in locali ad accesso controllato, utilizzando armadi o cassetti chiusi a chiave.

Trattamenti con l'ausilio di mezzi elettronici

Al fine di poter trattare i dati mediante dispositivi informatici, deve essere prevista una procedura di autenticazione che consenta l'identificazione degli Incaricati autorizzati allo specifico trattamento, attraverso "credenziali di autenticazione". Esse consistono in un User-Id associato ad una parola chiave segreta (password) o in un dispositivo di autenticazione.

Le User-Id individuali per l'accesso alle applicazioni NON devono essere MAI condivise da più utenti (anche se incaricati del trattamento). Nel caso in cui occorresse permettere l'accesso da parte di altri utenti, è necessario richiedere l'autorizzazione al Titolare del trattamento.

Per i PC collegati in rete gli incaricati devono farsi identificare per poter accedere alle risorse presenti nella rete dell'azienda; nel caso di utilizzo di applicazioni centralizzate gli incaricati devono provvedere anche alla propria identificazione sul sistema applicativo centrale secondo le modalità e le regole previste dall'applicativo stesso.

Tutti gli incaricati che utilizzano un personal computer per il trattamento di dati personali non collegato in rete devono proteggere l'accesso alla propria postazione di lavoro attivando una password come previsto dalle funzionalità di protezione del BIOS del PC.

Gestione delle password

La scelta delle password da parte dell'autorizzato deve essere ponderata in quanto un utilizzo improprio della stessa è il modo più facile per un accesso illecito da parte di terzi alla rete e/o all'applicazione, e di conseguenza ai dati in essi custoditi a tutti gli effetti risultando con l'identità di un altro utente.

Una password deve essere facile da ricordare ma, allo stesso tempo, difficile da individuare. Questa sezione offre dei suggerimenti su come scegliere e proteggere la propria password. Queste linee guida rivestono un'importanza particolare se si lavora con materiale sensibile.
Nella gestione delle password è necessario osservare le seguenti indicazioni:

1. NON comunicare a NESSUNO le proprie password. Ricordare che nessuno è autorizzato a richiedere le password, nemmeno il personale tecnico di supporto.

2. NON scrivere le proprie password su supporti facilmente rintracciabili e soprattutto in prossimità della postazione di lavoro utilizzata.

3. NON scegliere password corrispondenti a parole presenti in un dizionario, sia della lingua italiana che di lingue straniere. Non utilizzare nemmeno parole del dizionario in senso inverso.

4. NON usare parole che possano essere facilmente riconducibili all'identità dell'utente come, ad esempio, il codice fiscale, il nome del coniuge o dei figli, la data di nascita, il numero di telefono, la targa della propria auto, il nome della via in cui si abita, il proprio numero di matricola o addirittura la stessa ID, ecc.

5. NON usare come password parole ottenute da una combinazione di tasti vicini alla tastiera o sequenze di caratteri.

6. NON usare la stessa password per l'accesso a sistemi ed applicativi differenti.

7. NON comunicare password vecchie e non più in uso in quanto potrebbe essere possibile ricavare da questi dati regole empiriche o personali che l'autorizzato utilizza per generare le proprie password.

8. Cambiare le password (almeno ogni sei mesi, tre per i trattamenti di dati sensibili) e comunque dentro i limiti previsti dalle misure minime di sicurezza.

9. Le password di accesso alle procedure informatiche che trattano dati di categorie particolari (sensibili o giudiziari) devono essere sostituite, da parte del singolo incaricato, almeno OGNI TRE MESI

10. Utilizzare password lunghe almeno 8 caratteri od il massimo consentito dal sistema utilizzando un misto di lettere, numeri e segni di interpunzione (Ad esempio: .;$!@-><£§).

11. Nel digitare la password accertarsi che non ci sia nessuno che osservi e sia in grado di vedere od intuire i caratteri digitati sulla tastiera

Come scegliere la password

Di seguito sono riportati alcuni suggerimenti per la formazione di password abbastanza sicure e facili da ricordare:

- Formare una parola senza senso.
- Formare un acronimo.
- Cambiare volontariamente l'ordine delle lettere di una parola o utilizzare simboli e numeri al posto di alcune lettere.
- Mettere insieme le sillabe da una canzone o una poesia preferite. Una tecnica può essere quella di comprimere frasi lunghe in pochi caratteri presenti nella frase, utilizzando segni di interpunzione e caratteri maiuscoli e minuscoli.

Suggerimenti utili in presenza di ospiti o terze parti

A conclusione del paragrafo si ribadisce come gli incaricati del trattamento debbono impedire l'accesso ai dati in loro possesso da parte di chi non è autorizzato. Qui si indicano poche regole di buona condotta che ogni Incaricato del trattamento di dati dovrebbe seguire in occasione di visite esterne o particolari situazioni di "minaccia" per la segretezza dei dati. Esse sono ad esempio

- Fare attendere gli ospiti in luoghi in cui non siano presenti informazioni riservate o dati personali.
- Se è necessario allontanarsi dalla scrivania in presenza di ospiti, riporre i documenti e attivare il salvaschermo del PC.
- Segnalare qualsiasi anomalia o stranezza di comportamento al Responsabile.

Sicurezza del software e dell'hardware

Le norme riportate in questa sezione sono finalizzate ad aumentare la sicurezza dei singoli sistemi informatici utilizzati per il trattamento dei dati. Il rispetto di tali norme garantisce anche che non vengano compromesse le misure di sicurezza del sistema informativo ad opera di un utente regolarmente autorizzato, ma che inconsapevolmente adotta comportamenti in grado di violare l'integrità del sistema (installazione inconsapevole di virus o di "trojan horse").

L'autorizzato non può installare sulla propria postazione di lavoro programmi non attinenti alle normali attività d'ufficio né nuovi programmi necessari senza la preventiva autorizzazione. Gli utenti non possono modificare le configurazioni hardware e software senza l'autorizzazione.

Se un autorizzato o un addetto responsabile rileva un problema nell'ambito dell'utilizzo del sistema informatico relativo al trattamento di dati in corso che può compromettere la sicurezza dei dati ne dà immediata comunicazione al Responsabile del trattamento. Quest'ultimo provvede ad inoltrare la comunicazione al responsabile informatico che analizza il problema segnalato ed adotta tutte le misure tecniche necessarie a risolverlo.

Gli utenti che hanno accesso alla rete Internet mediante un personal computer in ambiente Microsoft Windows, verificano sul sito ufficiale della Microsoft (http://www.microsoft.com), con cadenza almeno mensile, le correzioni software per problemi di sicurezza applicabili alla propria versione di sistema operativo. Utilizzando la funzione "Windows Update" del proprio sistema operativo Microsoft Windows è possibile rilevare la presenza di correzioni software per problemi di sicurezza, l'utente è tenuto a scaricare ed installare tali aggiornamenti sul proprio PC seguendo le indicazioni riportate sul sito Microsoft. Anche gli utenti di postazioni di lavoro non Windows (es.: Linux Redhat, Apple MacOS X, ecc.) hanno la possibilità di scaricare gli aggiornamenti e le correzioni del proprio sistema operativo, utilizzando funzioni analoghe presenti sulla propria macchina.

Protezione da virus informatici

I virus informatici rappresentano una delle minacce principali per la sicurezza dei sistemi informativi e dei dati in esso presenti. Un virus informatico può modificare e/o cancellare i dati in esso contenuti, può compromettere la sicurezza e la riservatezza di un intero sistema informativo, può rendere indisponibile tutto o parte del sistema, compresa la rete di trasmissione dati. Al fine di non aumentare il livello di rischio di contaminazione da virus è opportuno:

1. accertarsi che sul proprio computer sia sempre operativo il programma antivirus in uso nell'azienda, aggiornato e con la funzione di monitoraggio attiva;
2. sottoporre a controllo con il programma installato sul proprio PC, tutti i supporti di provenienza esterna prima di eseguire file in esso contenuti
3. accertarsi sempre della provenienza dei messaggi di posta elettronica contenenti allegati; nel caso in cui il mittente sia di origine a dubbi, cancellare direttamente il messaggio senza aprire gli allegati
4. non condividere con altri computer il proprio disco rigido o una cartella di file senza password di protezione in lettura/scrittura;

5. proteggere in scrittura i propri supporti contenenti programmi eseguibili e/o file di dati;
6. limitare la trasmissione tra computer in rete di file eseguibili e di sistema;
7. non scaricare da Internet programmi o file non inerenti l'attività lavorativa o comunque sospetti.

Utilizzo della rete Internet/Data Breach

Il sistema informativo ed i dati in esso contenuti possono subire gravi danneggiamenti per un utilizzo improprio della connessione alla rete Internet; inoltre, come detto, attraverso la rete possono essere introdotti nel sistema virus informatici e possono penetrare utenti non autorizzati. Al fine di evitare questi pericoli, è opportuno attenersi alle regole seguenti:

1. utilizzare la connessione ad Internet esclusivamente per lo svolgimento dei propri compiti istituzionali;
2. non diffondere messaggi di posta elettronica di provenienza dubbia;
3. NON utilizzare la casella postale assegnata dall'azienda per FINI PRIVATI E PERSONALI;
4. non utilizzare servizi di comunicazione e condivisione di file (condivisione P2P "peer-to-peer");
5. gli utenti devono essere a conoscenza degli articoli del codice penale 615 ter –"Accesso abusivo ad un sistema informatico e telematico", 615 quater – "Detenzione e diffusione abusiva di codici di accesso a sistemi informatici e telematica", 615 quinquies – "Diffusione di programmi diretti a danneggiare ed interrompere un sistema informatico", nonché del Decreto Legge 22 Marzo 2004 n. 72 convertito in legge con modificazioni dalla Legge 21 Maggio 2004 n. 128 (Legge Urbani) che sanziona la condivisione e/o fruizione di file relativi ad un'opera cinematografica od assimilata protetta da Diritti d'autore.

Si ribadisce il fatto che nessun utente della rete informatica è autorizzato ad installare sulla propria postazione di lavoro software non previsto dalla configurazione di base. È pertanto vietato effettuare il download e l'installazione dalla rete Internet, a meno che non sia stata data esplicita autorizzazione da parte dell'azienda.

Comunicazione data breach

Adempimenti previsti in capo agli Incaricati del trattamento dei dati

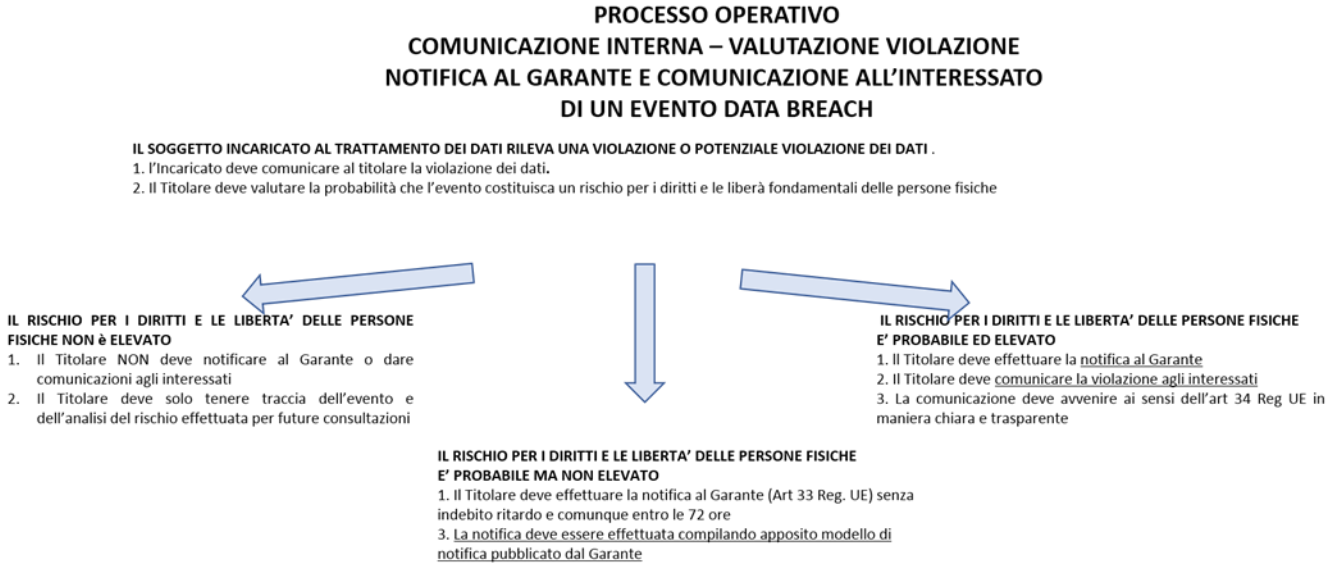
Il Data Breach consiste in una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Un Data Breach non è, quindi, solo un attacco informatico, ma può essere anche un accesso abusivo, un incidente (es. un incendio o una calamità naturale), la semplice perdita di una chiavetta USB o la sottrazione di documenti con dati personali (furto di un notebook di un dipendente).

Il Regolamento Europeo 679/2016 prescrive specifici adempimenti nel caso di una violazione di dati personali.

In particolare, il Regolamento prescrive l'obbligo, in capo al Titolare del trattamento dei dati, che ritiene probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, di comunicare al Garante per la protezione dei dati personali la violazione dei dati occorsa entro 72 ore e comunque "senza ingiustificato ritardo".

Gli autorizzati al trattamento dei dati (dipendenti/collaboratori) devono rilevare e segnalare tempestivamente al Titolare tutti gli episodi di tipo violazione dei dati.



Sanzioni per inosservanza delle norme

Le presenti istruzioni operative sono impartite ai sensi delle normative vigenti, l'inosservanza delle quali da parte dell'autorizzato può comportare sanzioni anche di natura penale a suo carico.