OPUSCOLO INFORMATIVO PER GLI INCARICATI AL TRATTAMENTO DEI DATI AI SENSI DELLA NORMATIVA SULLA PRIVACY

Sommario

1. INTRODUZIONE

Il presente opuscolo informativo contiene gli elementi basilari all'informazione in tema di protezione dei dati personali ai sensi dalla normativa vigente (Regolamento UE 2016/679) per gli incaricato al trattamento dei dati.

2. DIRITTO ALLA PROTEZIONE DEI DATI PERSONALI

La normativa specifica che "chiunque ha diritto alla protezione dei dati personali che lo riguardano". Sono oggetto del diritto le informazioni relative ad ogni persona fisica. La normativa in materia di privacy garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

3. ALCUNE DEFINIZIONI

Trattamento dei dati	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
Dati personali	Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica 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.
Categorie particolari di dati personali	I dati personali idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i 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.

4. L'ORGANIZZAZIONE AZIENDALE AI FINI DELLA PRIVACY E LE FIGURE DELLA PRIVACY

In merito ai soggetti che effettuano il trattamento dei dati la normativa prevede che "quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo, il titolare del trattamento è l'entità nel suo complesso" Il Titolare, può designare un Responsabile (o più responsabili) a cui affiderà compiti che devono essere analiticamente specificati per iscritto. Il Responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni e delle proprie istruzioni. La legge prevede la definizione di una serie di adempimenti e modalità atti ad assicurare che il sistema Privacy sia sotto controllo, operi correttamente e sia improntato su una organizzazione aziendale al cui vertice vi è il "Titolare del trattamento, ed a seguire i Responsabili dei vari trattamenti (figure che il titolare ha la facoltà, e non l'obbligo di designare), e gli incaricati del trattamento (tutte le persone, solitamente lavoratori dipendenti, che sono autorizzati a compiere operazioni di trattamento secondo le istruzioni impartite dal titolare o dal responsabile). L'incaricato del trattamento deve attenersi alle istruzioni impartite, per iscritto, dal Titolare e dal Responsabile del trattamento. Ogni comportamento contrario alle istruzioni impartite potrà essere oggetto di richiami o sanzioni da parte del titolare del trattamento

Le definizioni ai sensi della normativa vigente:

Titolare del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.
Responsabile del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.
Incaricati del trattamento	Le persone fisiche autorizzata a compiere operazioni di trattamento dai titolare o dal responsabile e che debbono attenersi alle istruzioni impartite dai titolare dal responsabile del trattamento

5. I DATI PRESENTI IN AZIENDA

Nell'ambito dell'attività di un'azienda sono trattati dati di clienti e fornitori ai fini dell'assolvimento di obblighi contabili e amministrativi, dati dei dipendenti e/o collaboratori dell'azienda ai fini della compilazione dei cedolini paga e dell'assolvimento degli obblighi in materia previdenziale.

In questa seconda tipologia si ricade nell'ipotesi di trattamento di dati "sensibili" dal momento che perverranno all'azienda certificati medici per malattie o certificati per infortuni, richieste di permessi per funzioni elettorali ai seggi, per festività religiose, certificati di gravidanza etc.

In azienda spesso si trattano altre tipologie di dati ad esempio i dati raccolti mediante la compilazione di un form all'interno del sito internet o alle banche dati acquisite all'esterno per intraprendere sulle stesse attività di marketing o, ancora, i dai raccolti in sede di colloquio di lavoro. Per differenti tipologie e finalità possono essere trattati altri dati personali, sensibili e non.

6. MODALITÀ, REQUISITI E PRINCIPI DI TRATTAMENTO DEI DATI

La normativa prevede espressamente che:

I dati personali oggetto di trattamento devono essere (art.5 GDPR 2016/679):

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»;
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
- esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione».

- trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

Inoltre è da ricordare che la norma prevede espressamente che "chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'art. 2050 del codice civile".

7. PRINCIPALI RISCHI A CUI SONO SOTTOPOSTI I DATI

I dati aziendali possono essere compromessi da una serie di eventi sia di carattere informatico sia fisico, che potrebbero comportarne la perdita o la distruzione, l'accesso non autorizzato o il trattamento non consentito o non conforme alle finalità della raccolta.
Durante i collegamenti esterni (internet, posta elettronica, scaricamento programmi dalla rete internet, extranet, ecc,) e i trasferimenti di dati da supporti di memorizzazione esterna si possono verificare degli accessi fraudolenti o dei trasferimenti di programmi informatici nel proprio sistema, che possono generare dei seri problemi all'integrità del sistema e dei dati in esso contenuti.
In particolare i pericoli si potrebbero verificare durante le seguenti operazioni:
• Aggiornamento dei programmi, trasferimento di files, ecc oppure utilizzando supporti di memorizzazione esterna (chiavette usb, unità esterna, CD, ecc);
• Navigazione in internet;
• Navigazione in extranet (rete di collegamento fra aziende esterne);
• Utilizzo della posta elettronica;
• Scaricamento (download) da internet di programmi o aggiornamenti di programmi (ad esempio aggiornamento dei programmi antivirus, ecc.);
• Collegamenti telematici con istituti di credito;
• Trasmissione di dati per via telematica ad enti pubblici.

In particolare per le attività sopra elencate si incorre nei seguenti rischi:

VIRUS INFORMATICI E VIOLAZIONE DELLA PRIVACY E DEI DATI CONTENUTI NEI PC (DATA BREACH)

I **virus informatici** sono programmi che possono intervenite sul software installato sui computer per attivare azioni, che possono distruggere, sottrarre o modificare completamente dati e/o programmi in esso. Una volta istallato nel proprio sistema, il virus può trasmettersi ad altri computer della rete aziendale o in fase di trasmissione files tramite posta elettronica.
I virus accedono agli elaboratori attraverso i seguenti mezzi:
- supporti di memorizzazione esterni utilizzati nel proprio sistema per trasferire i dati o programmi;
- a mezzo della posta elettronica quando si aprono i file allegati ai messaggi di altri utenti;
- scaricando programmi gratuiti dalla rete internet o contenuti in file ricevuti da terzi.

I **Trojan** sono programmi che hanno un comportamento simile a quelli dei virus ma non si replicano e non cercano di celarsi all'interno di altri programmi esistenti nel computer. Il "trojan" può entrare nei computer con le stesse modalità dei virus informatici e cioè tramite supporti esterni di memorizzazione, programmi o files copiati e posta elettronica.
I virus contenuti nelle macro si avvalgono della possibilità che hanno alcuni programmi gestionali (ad esempio excel, word, access) di permettere all'utente di inserire nei file di lavoro delle facili istruzioni simili ad un linguaggio di programmazione con le quali, è possibile replicare una serie di operazioni che si utilizzano spesso. Queste funzioni sì chiamano "macro". Tale possibilità può essere utilizzata dall'utente fraudolento per inserire in un file di lavoro delle istruzioni che possono cancellare una directory dei computer, spegnere il computer mentre si lavora ecc.. Il file modificato, una volta aperto nel proprio computer può eseguire automaticamente azioni dannose sul sistema.

Attraverso il collegamento ad Internet gli hacker, mediante appositi programmi informatici, possono accedere ai dati presenti nel PC e danneggiare i contenuti dei nostri archivi o appropriarsi dei dati personali presenti. La normativa prescrive l'adozione di severe misure minime di sicurezza per evitare i rischi e proteggere gli archivi delle aziende.

Un ulteriore rischio per i dati presenti in aziende è l'installazione nel nostro computer di istruzioni dette "cookies" che rimangono registrate nell'elaboratore e permettono ai web master di riconoscere il visitatore (ad esempio la data e l'ora della vostra ultima visita, una informazione personale contenuta nell'elaboratore, la frequenza delle viste, ecc).
I programmi Apple Java e controlli ActiveX sono utilizzati per migliorare la visualizzazione dei siti internet. Se i siti sono sicuri non esiste nessun problema, altrimenti, possono permettere l'accesso ai dati contenuti nel nostro computer.

RISCHI FISICI

Oltre ai rischi derivanti dalla possibilità di accesso informatico dall'esterno o dai virus informatici, la legge prevede anche la protezione fisica di aree e locali in cui sono installati i computer e gli archivi cartacei che contengono dati personali. La legge prevede inoltre che si stabiliscano procedure per controllare l'accesso delle persone autorizzate e che siano stabili criteri per assicurare l'integrità dei dati.
I rischi possono essere, ad esempio:

A. Ingresso non autorizzato di terzi nelle aree o nei locali con il fine di danneggiare il sistema o prelevare o visionare i dati sensibili contenuti negli elaboratori.

B. Incendio nei locali con distruzione dei PC e perdita definitiva dei dati in essi contenuti.

C. Eventi naturali quali l'allagamento dei locali (dovuto al alluvioni, rottura tubazioni, ecc) con conseguente danneggiamento dei computer e probabile perdita dei dati in essi contenuti.

Occorre quindi procedere all'adozione dei misure di sicurezza che consentano di contrastare i pericoli ed i rischi sopra evidenziati.

8. LE MISURE DI SICUREZZA

Rispetto alla disciplina previgente resta immutato il principio, secondo cui "*i dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati o alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento no consentito o non conforme alle finalità della raccolta*".

A tale scopo si richiede che il "Titolare del trattamento dei dati" adotti idonee misure di sicurezza, tenendo conto anche della natura dei dati e delle caratteristiche del trattamento.

Il codice distingue comunque tra trattamento effettuato con o senza l'ausilio di strumenti elettronici.

Le misure variano, divenendo sempre più severe, a seconda della tipologia dei dati trattati siano essi comuni o sensibili.

8.1 TRATTAMENTO EFFETTUATO <u>CON L'AUSILIO DI MEZZI ELETTRONICI</u>

Di seguito si indicano le misure minime previste dalla normativa sulla privacy per i trattamenti effettuati con l'ausilio di strumenti elettronici, in relazione alle modalità tecniche di attuazione contenute nel Disciplinare Tecnico.

SISTEMA DI AUTENTICAZIONE INFORMATICA

Il codice distingue fra procedure di autenticazione e di autorizzazione: ai sensi del disciplinare tecnico, il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione.

Le credenziali di autenticazione possono semplicemente consistere in un codice per l'identificazione dell'incaricato associato ad una parola chiave (username + password).

Sono inoltre specificate le caratteristiche che deve possedere la parola chiave (almeno otto caratteri o, se lo strumento elettronico non lo permette, il numero massimo di caratteri consentito), la sua durata massima (la parola chiave deve essere immediatamente modificata dal singolo incaricato al momento dell'assegnazione e successivamente modificata, sempre dall'incaricato, almeno ogni 6 mesi per i dati comuni ed ogni 3 mesi se si effettua trattamento di dati sensibili o giudiziari) l'eventuale sua disattivazione (nel caso di non utilizzo prolungato per sei mesi o, chiaramente, in caso di vicende che riguardino direttamente l'incaricato).

Resta fermo l'obbligo per il Titolare di impartire agli Incaricati del Trattamento idonee e preventive informazioni scritte circa l'utilizzo degli strumenti elettronici, l'adozione di adeguate cautele.

A tal fine, permane la figura del custode delle credenziali (o custode delle parole chiave), preventivamente individuato per iscritto.

SISTEMA DI AUTORIZZAZIONE

L'autorizzazione agli incaricati costituisce invece una fase distinta e successiva rispetto all'autenticazione. L'autorizzazione consente, infatti, al singolo incaricato di accedere a determinate categorie di dati. È evidente che i profili di autorizzazione dovranno essere individuati all'inizio del trattamento stesso nell'ambito dell'assegnazione e delle istruzioni scritte fornite agli incaricati.

ALTRE MISURE DI SICUREZZA

Fra le ulteriori misure, si segnala l'obbligo, da parte del Titolare del Trattamento di:

- ✓ INSTALLARE PROGRAMMI ANTIVIRUS
- ✓ INSTALLARE SISTEMI ANTINTRUSIONE (Firewall)
- ✓ INSTALLARE PROGRAMMI ATTI A PREVENIRE LA VULNERABILITA' DEGLI STRUMENTI ELETTRONICI E A CORREGGERE I DIFETTI;
- ✓ EFFETTUARE IL SALVATAGGIO DEI DATI (back up) CON FREQUENZA ALMENO SETTIMANALE;
- ✓ SEGUIRE SPECIFICHE DISPOSIZIONI PER LA RIUTILIZZAZIONE O LA DISTRUZIONE DEI SUPPORTI RIMOVIBILI CONTENENTI DATI SENSIBILI.

8.2. TRATTAMENTO SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Si dovranno impartire agli incaricati istruzioni scritte finalizzate al controllo ed alla custodia degli atti e dei documenti contenenti dati personali. Atti e documenti contenenti dati sensibili o giudiziari sono affidati agli incaricati dei trattamento, che li controllano e li custodiscono fino ai termine delle operazioni. L'accesso agli archivi contenenti dati sensibili o giudiziali è controllato e le persone ammesse sono identificate e registrate.

9. VERIFICHE PERIODICHE

Il titolare del trattamento dei dati personali dovrà svolgere le seguenti operazioni:

- ✓ Verificare che la normativa sulla privacy venga rispettata;
- ✓ Verificare che i "Responsabili" del trattamento garantiscano, nell'ambito della funzione e dei compiti loro assegnati, il rispetto pieno delle istruzioni loro fornite in materia di trattamento dei dati;
- ✓ Verificare che gli "Incaricati" del Trattamento, gestiscano i dati ai quali hanno accesso attenendosi alle istruzioni loro fornite da parte del titolare stesso o del responsabile;
- ✓ Valutare l'efficacia delle misure di sicurezza adottate ed apportare le modifiche eventualmente necessarie.

10. MODALITA' DI UTILIZZO DEGLI STRUMENTI ELETTRONICI AZIENDALI

È vietato, in azienda, l'uso dei dispositivi informatici per finalità diverse da quelle dell'organizzazione e per scopi personali.

Qui di seguito vengono elencate, in modo esemplificativo, le principali disposizioni alle quali ciascun incaricato dovrà attenersi scrupolosamente.

L'azienda si riserva comunque il diritto, in qualsiasi momento, di attuare specifiche disposizioni aziendali o disciplinari, ai fini di una maggiore regolamentazione di trattamento dei dati aziendali.

Tutti gli incaricati, avranno l'obbligo di:

- Non comunicare la password scelta a colleghi o altro personale, fatta salva la comunicazione scritta al custode delle credenziali;

- Non lasciare incustodito e accessibile il PC durante le 'operazione di trattamento dei dati adoperandosi, in caso, ad attivare lo screensaver protetto da password;

- Non installare sullo strumento informatico affidato alcun programma, senza preventiva autorizzazione del Titolare o del/dei responsabile/i del trattamento;

- Non effettuare il download di programmi o file da siti internet, se non previa autorizzazione del titolare o dei/dei responsabile/i del trattamento, fatta eccezione per i download che eventualmente vengano eseguiti per l'aggiornamento di programmi abituali installati ed in uso;

- Astenersi dalla consultazione di siti internet i cui contenuti non siano di utilità ai finì dello svolgimento dei compiti affidati;

- Utilizzare la casella di posta elettronica a fini esclusivamente aziendali;

- Astenersi dall'aprire messaggi da mittenti non conosciuti, che potrebbero contenere virus;

- Utilizzare, solo se indispensabile, supporti rimovibili, hard disk, pen drive, cd-rom e dvd.

11. LE SANZIONI

Si informa che la non osservanza delle prescrizioni contenute costituisce grave violazione delle disposizioni normative con la possibile applicazione di sanzioni civili e penali oltre che disciplinari.