Circolare informativa sulla Privacy

Com'è ormai noto, il Codice sulla tutela dei dati personali (D. Lgs. n. 196/2003) ha ridisegnato il sistema degli adempimenti amministrativi, organizzativi e delle misure di sicurezza, la cui osservanza viene imposta ai titolari dei trattamenti anche attraverso il ricorso a sanzioni penali e a pesanti sanzioni amministrative.
Si fornisce un estratto delle principali **misure da adottare** e dei **documenti da predisporre e conservare** ricordando che per quel che concerne gli adeguamenti informatici e tecnici sarà necessario, per chi non è in grado di operare direttamente, rivolgersi ai propri tecnici di fiducia.

N.B. più avanti si potrà far riferimento ai c.d. "dati sensibili": si ricorda che tali dati sono identificati come tutti quei dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

PUNTO 1° - NOTIFICA AL GARANTE E AUTORIZZAZIONE

Il trattamento dei dati sensibili è stato autorizzato d'ufficio con provvedimento di carattere generale dal Garante per il trattamento dei dati sensibili: i) nei rapporti di lavoro; ii) idonei a rilevare lo stato di salute e la vita sessuale; iii) da parte degli enti associativi e fondazioni; iiii)da parte dei liberi professionisti; iii) da parte di altre categorie meno comuni. I titolari di queste categorie non sono tenuti a chiedere l'autorizzazione al Garante.
Tali esoneri dovrebbero essere sufficienti per evitare la notifica nella maggior parte dei casi.

PUNTO 2° - INFORMATIVA

La persona fisica o giuridica di cui si trattano i dati ha il diritto di essere informato sia del trattamento stesso sia dei modi e delle finalità per cui è effettuato. Tale informativa (che la legge prevede possa essere anche resa verbalmente, metodo che però non appare sufficientemente sicuro), deve essere fatta firmare ogni qual volta si entri in contatto per la prima volta con un nuovo cliente, dipendente, collaboratore ecc..
L'informativa dovrà essere resa anche ai fornitori che a loro volta la raccolgono da noi.
A questo proposito alleghiamo un **esempio di informativa (vedi informativa clienti)** ricordando che le stesse vanno conservate fino a che si conservano i dati relativi a quell'interessato. Resta comunque valida (specialmente quando si corre il rischio di dimenticarsi della raccolta di un'informativa preventiva) l'adozione di una apposita frase direttamente in fattura pertinente solo alla fase di vendita.
Alleghiamo alla presente anche un **esempio di informativa** da rendere **ai dipendenti (vedi informativa dipendenti)** facendo però presente che solitamente tale informativa è predisposta e conservata dal consulente delle paghe e che sarà quindi meglio contattarlo prima di procedere all'espletamento di tale onere.

PUNTO 3° - IDENTIFICAZIONE DEL TITOLARE DEL TRATTAMENTO

La persona fisica o la persona giuridica cui compete le decisioni in ordine alle finalità, modalità del trattamento dei dati personali e agli strumenti utilizzati viene identificato come **"Titolare del trattamento"** .

PUNTO 4° - NOMINA DEL RESPONSABILE DEL TRATTAMENTO

Il titolare del trattamento di cui al punto precedente nominerà uno o più responsabili **(vedi responsabile)** i quali vigileranno sul corretto utilizzo degli archivi e sulla loro conservazione. La nomina del responsabile è facoltativa ma è bene che l'Amministratore unico, il Presidente del C.d.A. o il legale rappresentante venga nominato a questo incarico al fine di evitare che eventuali responsabilità possano ricadere sui dipendenti e/o collaboratori che si occupano quotidianamente del trattamento dei dati ai fini contabili-fiscali.

PUNTO 5° - ALTRE NOMINE

Nomina degli incaricati al trattamento dei dati

Il Responsabile del trattamento nominerà e autorizzerà per iscritto tutte le persone addette all'utilizzo degli archivi cartacei e/o elettronici. L'autorizzazione potrà essere generale o limitata ad alcuni specifici dati e programmi e dovrà essere rilasciata prima dell'inizio del trattamento.
Tali autorizzazioni dovranno essere verificate almeno una volta l'anno e se necessario modificate (es. contabile amministrativo che viene promosso a responsabile vendite/acquisti ecc.). Verrà poi redatto un apposito elenco di tutti gli incaricati che comprenderà, dove sia utilizzata una rete di computer, lo User-Id che identifica il PC utilizzato da ognuno.
Ad ogni incaricato dovranno essere assegnate delle password **univochee non riutilizzabili** sia per entrare all'interno del programma sia per riprendere l'uso del pc dopo essersi allontanato (c.d. screen-saver). Tali password, che dovranno essere di almeno otto caratteri, dovranno essere conservate diligentemente da ogni incaricato e dallo stesso modificate almeno ogni sei mesi (ridotti a tre per gli incaricati al trattamento dei dati sensibili).
Le password non utilizzate da almeno 6 mesi (es. maternità di un dipendente) e quelle non più utilizzate (es. ex dipendente) devono essere disattivate.

Custode delle Password

Il Responsabile del trattamento nominerà un Custode delle Password che sarà l'unico a conoscere tutte le password, oltre naturalmente al singolo incaricato che sarà a conoscenza solo della propria, e provvederà a controllare che le password siano univoche. Egli predisporrà tante buste chiuse quanti sono gli incaricati al trattamento. Tali buste, riconoscibile all'esterno da nome dell'incaricato, conterranno le password (vedi documento 6bis) e dovranno essere custodite in posto sicuro e non accessibile. Quando uno o più incaricati dovessero variare, il Custode provvederà a distruggere la/le relativa/e buste ed eventualmente, se necessario, a predisporne delle nuove per i nuovi incaricati ricordandosi sempre che una parola chiave già utilizzata non può essere riassegnata ad un nuovo utente. Il procedimento fin qui descritto deve essere effettuato anche in presenza di un solo PC.

Amministratore di sistema

Dove sia utilizzata una rete o vi siano più elaboratori, è necessario che il Responsabile nomini un Amministratore di sistema incaricato del controllo dei trattamenti effettuati elettronicamente. L'Amministratore di sistema provvederà anche, ogni sei mesi al massimo, ad archiviare un documento da lui firmato e datato in cui segnalerà quanto fatto al fine dell'adeguamento e/o dell'aggiornamento dei sistemi antivirus. Provvederà inoltre, in presenza di dati sensibili, ad adottare idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici nel tempo massimo previsto in sette giorni.
Ove, per mancanza dei presupposti, non si renda necessaria la nomina di un amministratore di sistema, il documento relativo agli antivirus dovrà comunque essere compilato e conservato a cura di uno dei responsabili del trattamento.

PUNTO 6° - DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Entro il 31 marzo di ogni anno ed in presenza di dati sensibili, il titolare del trattamento dovrà redigere un documento programmatico sulla sicurezza **(vedi documento n. 10)** in cui verranno elencati tutti i provvedimenti presi e gli adeguamenti effettuati al fine della tutela sulla Privacy.

Con l'art. 34 comma 1-bis del D.Lgs 196/2003 e provvedimento del Garante del 27-11-2008 sono state introdotte ulteriori misure di semplificazione come segue:
a) Soggetti che trattano esclusivamente dati personali non sensibili, quando gli unici dati sensibili di cui sono in possesso sono quelli relativi allo stato di salute o di malattia dei propri dipendenti o collaboratori, senza indicazione della relativa diagnosi, oppure all'adesione ad organizzazioni sindacali o a carattere sindacale.
Per questi soggetti è prevista l'abolizione dell'obbligo di tenere un aggiornato documento programmatico della sicurezza (DPS) e dalla sua sostituzione con una **autocertificazione**, resa ai sensi dell'art. 47 del D.P.R 445/2000, con la quale il titolare dovrà dichiarare di:
1.trattare generalmente solo dati personali non sensibili
2.essere in possesso dei soli dati sensibili previsti
3.trattare, comunque, questi ultimi nell'osservanza delle misure di sicurezza previste dal codice e dall'allegato B.
Attenzione:
1.l'obbligo del DPS decade soltanto se risultano trattati dati sensibili della stessa specie di quella prevista , mentre in presenza anche di un solo altro dato sensibile di natura differente (ad es. quelli relativi all'adesione a partiti politici, organizzazioni di carattere religioso, ecc...) tutto rimane come prima;
2.non viene meno l'obbligo di applicare le altre misure di sicurezza previste;
3.l'autocertificazione non è un semplice adempimento burocratico, poichè in caso di false attestazioni (ad es. sulla natura dei dati trattati e/o sull'osservanza delle misure di sicurezza) comporta una responsabilità da parte del titolare dei dati;
b) Piccole e medie imprese, liberi professionisti, artigiani, che non rientrano nella prima categoria, e che comunque limitano i trattamenti alle ormai leggendarie *correnti finalità amministrative e contabili.* A costoro, esclusi dall'autocertificazione, il legislatore concede la possibilità di compilazione di un **documento programmatico della sicurezza (DPS) semplificato.**

Il Titolare dovrà inoltre **riferire** della redazione o dell'aggiornamento di tale documento **nella relazione accompagnatoria al bilancio** (quando prevista).

PUNTO 7° - ADOZIONE MISURE DI SICUREZZA

Devono essere adottare le misure minime di sicurezza previste dal disciplinare tecnico allegato al Codice della Privacy. Tali misure possono essere così adempiute:

Misure "minime" di sicurezza per i trattamenti senza strumenti elettronici

Qualora il trattamento di dati personali sia effettuato senza l'ausilio di strumenti elettronici (es. archivi cartacei), ai sensi dell'art. 35 del Codice occorre adottare le seguenti misure minime di sicurezza:
• aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
• previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
• previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.
Le disposizioni attuative sono contenute nelle regole 27-29 del disciplinare tecnico, allegato B) del Codice.

Istruzioni scritte
Agli incaricati devono essere impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.
Con cadenza almeno annuale deve essere aggiornata l'individuazione dell'ambito del trattamento consentito ai singoli incaricati; la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

Atti e documenti contenenti dati personali "sensibili" o giudiziari
Quando gli atti e i documenti contenenti dati personali "sensibili" o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati, fino alla restituzione, in maniera che ad essi non accedano persone prive di autorizzazione e sono restituiti al termine delle operazioni affidate.
Non è però più espressamente richiesto che i suddetti atti e documenti siano conservati in contenitori muniti di serratura.

Accesso agli archivi contenenti dati personali "sensibili" o giudiziari
L'accesso agli archivi contenenti dati "sensibili" o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate.

Misure "minime" di sicurezza per i trattamenti mediante strumenti elettronici

Ai sensi dell'art. 34 del Codice, il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, a cura del titolare, del responsabile ove designato e dell'incaricato, le seguenti misure minime:
• autenticazione informatica;
• adozione di procedure di gestione delle credenziali di autenticazione;
• utilizzazione di un sistema di autorizzazione;
• aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
• protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
• adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
• tenuta di un aggiornato documento programmatico sulla sicurezza;
• adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Sistema di autenticazione informatica
Ai sensi dell'art. 4 co. 3 lett. c) del Codice, l'"autenticazione informatica" è "l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità".

Le disposizioni specifiche relative all'autenticazione informatica sono contenute nelle regole 1-11 del disciplinare tecnico, allegato B) del Codice.

Credenziali di autenticazione
Ai sensi dell'art. 4 co. 3 lett. d) del Codice, le "credenziali di autenticazione" sono "i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica".
Le credenziali di autenticazione consistono:
- in un codice per l'identificazione dell'incaricato (es. login, PIN, username, ecc.) associato a una "parola chiave" (password) riservata e conosciuta solamente dal medesimo;
- oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato (es. una smart card), eventualmente associato a un codice identificativo o a una parola chiave;
- oppure in una caratteristica biometrica dell'incaricato (es. impronta digitale), eventualmente associata a un codice identificativo o a una parola chiave.

Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione; l'incaricato deve adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo.
Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
Le credenziali di autenticazione sono disattivate:
- se non utilizzate da almeno sei mesi, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica;
- in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante l'uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici 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. In tal caso, la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

"Parole chiave"
Ai sensi dell'art. 4 co. 3 lett. e) del Codice, la "parola chiave" è la "componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica".
La "parola chiave":
- è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
- non deve contenere riferimenti agevolmente riconducibili all'incaricato. Pertanto, non sembrano quindi idonee le password costituite, ad esempio, dal nome o dalla data di nascita propria o di un familiare; una buona password, inoltre, dovrebbe contenere sia dati alfabetici che numerici;
- è modificata dall'incaricato al primo utilizzo e, successivamente, almeno ogni sei mesi (tre mesi in caso di trattamento di "dati sensibili" o giudiziari).

Le disposizioni sul sistema di autenticazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

"Sistema di autorizzazione"
Ai sensi dell'art. 4 co. 3 lett. g) del Codice, il "sistema di autorizzazione" è "l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente".
Ai sensi della precedente lett. f), il "profilo di autorizzazione" è "l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti".
Le disposizioni specifiche relative al sistema di autorizzazione sono contenute nelle regole 12-15 del disciplinare tecnico, allegato B) del Codice.
I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.
Le disposizioni sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

Programmi "antivirus" e loro aggiornamento
La regola 16 del disciplinare tecnico, allegato B) del Codice, stabilisce che i dati personali devono essere protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale (c.d. "virus"), mediante l'attivazione di idonei strumenti elettronici (c.d. "programmi antivirus") da aggiornare con cadenza almeno semestrale.
Aggiornamento dei software
La regola 17 del disciplinare tecnico, allegato B) del Codice, stabilisce che almeno annualmente, ovvero ogni sei mesi in caso di trattamento di "dati sensibili" o giudiziari, occorre effettuare aggiornamenti periodici dei programmi per elaboratore, volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti.

Il "back-up" periodico
La regola 18 del disciplinare tecnico, allegato B) del Codice, prevede il salvataggio dei dati (c.d. "back-up") con frequenza almeno settimanale.

Documento programmatico sulla sicurezza
La regola 19 del disciplinare tecnico, allegato B) del Codice, prevede l'obbligo di redazione di un "documento programmatico sulla sicurezza" (DPS).
I presupposti per l'obbligo di redazione del documento
L'obbligo di redazione del documento programmatico sulla sicurezza ricorre in caso di trattamento di dati personali "sensibili" o giudiziari con strumenti elettronici (es. computer).
Si ricorda che, in base alla disciplina anteriore al Codice della privacy (art. 6 del DPR n. 318/99), il documento programmatico sulla sicurezza doveva essere predisposto e aggiornato da parte dei soggetti che trattavano dati "sensibili" o dati giudiziari per mezzo di computer accessibili da altri computer "mediante una rete di telecomunicazioni disponibili al pubblico".

Il soggetto obbligato alla redazione del documento
Soggetto obbligato alla redazione del documento programmatico sulla sicurezza è il titolare dei suddetti trattamenti, anche attraverso il responsabile se designato.

Contenuto
Il documento programmatico sulla sicurezza contiene idonee informazioni riguardo:
- all'elenco dei trattamenti di dati personali;
- alla distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- all'analisi dei rischi che incombono sui dati;
- alle misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché alla protezione delle aree e dei locali, rilevanti ai fini della loro

custodia e accessibilità;
- alla descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- alla previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare; la formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
- alla descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al Codice, all'esterno della struttura del titolare;
- per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, all'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Nel **DPS semplificato** devono essere date informazioni riguardanti: (i) le coordinate identificative del titolare del trattamento, nonché, se designati, gli eventuali responsabili, (ii) una descrizione generale del trattamento o dei trattamenti realizzati, (iii) l'elenco, anche per categorie, degli incaricati del trattamento e delle relative responsabilità, (iv) una descrizione delle altre misure di sicurezza adottate per prevenire i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Termini di redazione o aggiornamento
Il documento programmatico sulla sicurezza, anche semplificato, deve essere redatto o aggiornato entro il 31 marzo di ogni anno. Anche l'autocertificazione, in caso di esonero dalla compilazione del DPS, deve essere predisposta entro il 31 marzo.

L'indicazione nella relazione accompagnatoria del bilancio d'esercizio
La regola 26 del disciplinare tecnico, allegato B) del Codice, prevede che "il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza".
Tale indicazione deve avvenire: (i) sia quando il documento programmatico della sicurezza sia obbligatorio come misura "minima", (ii) sia quando venga comunque adottato come "idonea" misura di sicurezza.

Le altre misure di sicurezza in caso di trattamento di dati "sensibili" o giudiziari
Le regole 20-24 del disciplinare tecnico, allegato B) del Codice, stabiliscono che in caso di trattamento di dati "sensibili" o giudiziari occorre altresì:
- proteggere i dati contro l'accesso abusivo mediante l'utilizzo di idonei strumenti elettronici;
- impartire istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti; i supporti rimovibili se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e non sono tecnicamente ricostruibili in alcun modo;
- adottare idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

La certificazione da parte degli installatori
Infine, con la regola 25 del disciplinare tecnico, allegato B) del Codice, viene stabilito che, qualora l'adozione di misure minime di sicurezza avvenga avvalendosi di soggetti esterni, il titolare deve ricevere dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni dello stesso disciplinare tecnico.

Seregno, 2 gennaio 2010

Studio Contrino.