

Data Security

La privacy e le aziende

- ✓ **Il Documento Programmatico sulla Sicurezza**
- ✓ **L'organizzazione della privacy**
- ✓ **La formazione**
- ✓ **Le sanzioni**
- ✓ **Come ottemperare alle disposizioni di legge**
- ✓ **Profilo di Data Security**

Il 1° Gennaio 2004 è entrato in vigore il nuovo codice privacy e di conseguenza anche il quadro delle misure minime di sicurezza che devono essere adottate nel trattamento dei dati personali, che è profondamente cambiato rispetto a quello previsto dalla vecchia legge 675/96 e dal Dpr 318/99.

Il **Disciplinare tecnico in materia di misure minime di sicurezza**, che entra a fare parte integrante del nuovo codice privacy, prevede diverse novità sostanziali ed è quindi importante avere ben chiare quali sono le misure da adottare per tutti le Aziende e verificare la propria situazione per ottemperare ai dettami della nuova legge ed evitare di incorrere nelle pesanti sanzioni previste per coloro che non le rispettano.

I controlli effettuati dal Garante hanno evidenziato come solo il 48% delle aziende controllate sia in regola con gli adempimenti privacy. Crediamo quindi di fare un'operazione utile e gradita nel segnalarvi brevemente quali sono i punti importanti da tener presente in vista dell'entrata in vigore delle nuove norme e di mettere a vostra disposizione l'esperienza e la professionalità che da anni contraddistinguono Data Security nei servizi di consulenza per la sicurezza e la privacy.

Naturalmente a problematica relativa alla privacy e alla sicurezza delle informazioni non si esaurisce nei punti descritti in questo documento, ma si articola nelle diverse peculiarità ed esigenze che contraddistinguono l'attività delle singole aziende.

IL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Come sottolineato, l'obbligo di redigere il Documento Programmatico sulla Sicurezza viene esteso a tutti in casi in cui si trattino dati sensibili o giudiziari con l'utilizzo di strumenti elettronici, anche nell'ipotesi in cui tali strumenti non siano in rete. È quindi sufficiente che tali dati siano trattati anche con un singolo elaboratore, perché si debba procedere alla redazione del documento.

Viene inoltre fissato una scadenza per la redazione e l'aggiornamento, che devono essere effettuati entro il 31 marzo di ogni anno.

Il punto 19 del Disciplinare tecnico prescrive che il DPS debba contenere idonee informazioni riguardo:

- l'elenco dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- la 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;

- la 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, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Oltre ad essere un obbligo di legge, il DPS ha anche una importante funzione interna di guida alla adozione ed al miglioramento delle misure di sicurezza: è quindi opportuno concepirlo come un vero e proprio piano per la sicurezza, estendendo il suo contenuto a tutti gli aspetti legati a tale problematica, che vanno anche oltre gli elementi obbligatori prescritti dal disciplinare tecnico.

Il DPS costituisce inoltre il punto di partenza per definire interventi e strategie per la sicurezza dei dati, perché permette di verificare il livello della sicurezza informatica e quindi di identificare subito le aree maggiormente a rischio. La specificità delle strutture nei diversi soggetti fanno sì che il DPS non sia un documento uguale per tutti, ma il frutto di una valutazione specifica da parte delle singole aziende, congiuntamente ai propri consulenti.

Certo la stesura del Documento Programmatico sulla Sicurezza è un'attività che richiede esperienza e competenze specifiche, senza le quali si corre il rischio di ridurre l'operazione ad un'inutile attività burocratica. Data Security, grazie alla competenza dei suoi consulenti e a una esperienza consolidata in decine di DPS in aziende e enti pubblici, può garantire il supporto in tutte le fasi di redazione, aggiornamento e certificazione del Documento Programmatico sulla Sicurezza.

E se, come spesso accade, nella fase di verifica viene riscontrata la necessità di provvedimenti urgenti, Data Security è attrezzata a fornire soluzioni chiavi in mano in grado di assicurare a pieno il rispetto dei requisiti di legge e gli standard internazionali per la sicurezza informatica.

L'ORGANIZZAZIONE DELLA PRIVACY

La prima e più urgente misura di sicurezza è quindi quella di carattere organizzativo. Il processo della sicurezza richiede infatti che, prima ancora di pensare all'adozione delle misure concrete, vengano definite una serie di compiti e procedure che regolino gli aspetti organizzativi del trattamento dei dati personali effettuato dall'Azienda.

È quindi necessario procedere preventivamente alla definizione di ruoli, compiti e responsabilità per la gestione di tutte le fasi del trattamento dei dati personali, con particolare riferimento alla necessità di garantire la loro sicurezza e alla adozione di specifiche procedure, che vadano a completare e rafforzare le contromisure tecnologiche adottate.

I consulenti Data Security possono affiancare i responsabili dell'organizzazione per la privacy all'interno dell'azienda per tutte le procedure di nomina, di approntamento di regolamenti, per la redazione di convenzioni per la comunicazione dei dati ad altre aziende private e ad enti pubblici e per stabilire le più adeguate policy di sicurezza.

LA FORMAZIONE

Il nuovo Codice sulla Privacy sancisce ancora una volta l'obbligatorietà di interventi formativi per gli incaricati del trattamento dei dati personali, già prevista dalla legge 675/96, dal D.P.R. 318/99 e dalle altre disposizioni in materia di privacy.

La legge prescrive di effettuare corsi per:

- informare gli incaricati del trattamento sui rischi che possono compromettere la sicurezza e la privacy dei dati;
- descrivere le misure di sicurezza disponibili per prevenire eventi dannosi;
- rendere edotti gli incaricati dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività;
- approfondire le responsabilità che ne derivano e le modalità per aggiornarsi sulle misure minime adottate dal titolare.

Questa formazione dovrebbe essere 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.

A questo scopo Data Security ha messo a punto e collaudato in diverse realtà, pubbliche e private, un **Corso per gli Incaricati del Trattamento dei dati personali** che illustra le responsabilità legate alle proprie funzioni, i rischi che minacciano i dati, le misure di sicurezza necessarie e i provvedimenti che tutte le aziende devono adottare.

Gli interventi formativi, sempre personalizzati per essere realmente coerenti con le prassi specifiche adottate in azienda, aiutano le diverse figure a conoscere meglio i rischi tipici nella gestione di dati personali e sensibili e le misure da adottare per ridurre i rischi e per ottenere un ragionevole livello di sicurezza e di privacy.

Oltre che per gli incaricati, infatti, la formazione sui temi della sicurezza e della privacy è utile anche per i Responsabili del trattamento dei dati, per i Dirigenti e gli Amministratori dell'azienda. Per queste figure sono a disposizione sessioni formative personalizzate che si focalizzano maggiormente sulle responsabilità specifiche dei ruoli dirigenziali.

ATTENZIONE ALLE TELECAMERE

Tra le sanzioni comminate fino ad oggi, la percentuale maggiore riguarda problematiche legate a telecamere per la videosorveglianza.

L'utilizzo di telecamere, spesso molto utile e funzionale in molte occasioni, deve sempre essere corredato da una attenta analisi di una serie di fattori rilevanti in termini di privacy, quali una verifica preliminare delle finalità a cui sono preposte, se il loro utilizzo è autorizzato, se è necessaria la notificazione al Garante. Anche per le telecamere vanno individuati Responsabili e Incaricati preposti al trattamento dei dati e alle misure di sicurezza.

Bisogna poi porre sempre apporre adeguati cartelli informativi e documentare le scelte fatte in termini di installazione delle telecamere, scelta dell'angolo visuale, tempi e modi di conservazione delle immagine ed implementazione delle misure di sicurezza previste.

INFORMATIVE E DIRITTI DELL'INTERESSATO

Altro adempimento previsto dalla normativa è quello di predisporre adeguate informative che illustrino ai cittadini le modalità di trattamento dei loro dati da parte dell'Azienda e, dove previsto, ne raccolgano il consenso al trattamento.

LE SANZIONI

“Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'**arresto sino a due anni** o con l'**ammenda da 10.000 euro a 50.000 euro**”(Art. 69)

Così recita il Decreto legislativo 30 giugno 2003, n. 196 per la mancata adozione delle misure di sicurezza ricordate nell'art. 34 per quanto riguarda il trattamento con strumenti elettronici:

- a) autenticazione informatica;
- b) adozione di procedure di gestione delle credenziali di autenticazione;
- c) utilizzazione di un sistema di autorizzazione;
- d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- g) tenuta di un aggiornato documento programmatico sulla sicurezza;
- h) 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.

e nell'art.35 per quanto riguarda i trattamenti senza l'ausilio di strumenti elettronici:

- a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
- b) previsione di procedure per un'adeguata custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
- c) 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.

Se poi dalla mancata od insufficiente adozione di idonee misure di sicurezza derivano danni a terzi, si è soggetti all'obbligazione del risarcimento, secondo i termini particolarmente severi previsti dalla legge.

Ai fini della responsabilità civile, inoltre, non è sufficiente porre in essere le misure *minime* di sicurezza previste dall'articolo 33 del codice, che sono invece sufficienti per non incorrere nelle disposizioni penali, ma si deve adottare misure *idonee*, con riferimento allo stato attuale della tecnologia.

Il che significa innanzitutto che ci si trova nel campo della **responsabilità oggettiva**, per cui il titolare del trattamento non risponde solo dei danni causati direttamente, ma anche di quelli provocati da tutti i propri dipendenti e persino da terzi, se non ha correttamente implementato le

giuste misure di sicurezza per impedirli.

Nel caso della privacy si applica infatti l'**inversione dell'onere della prova**: non è necessario che chi ha subito il danno debba provare la responsabilità oggettiva del titolare del trattamento, ma toccherà a questi provare di avere adottato *tutte le misure idonee* ad evitare il danno.

Il Garante per la Protezione dei dati personali ha inoltre intensificato l'attività ispettiva per verificare se i dati personali vengano trattati con correttezza e se le norme a tutela della privacy siano effettivamente rispettate da chi gestisce le banche dati.

Le ispezioni sono rivolte sia a soggetti privati che a pubbliche amministrazioni per accertare che i trattamenti di dati personali siano effettuati correttamente. Le ispezioni sono effettuate direttamente presso le sedi in cui vengono "trattati" i dati personali anche in collaborazione con il Nucleo speciale funzione pubblica e privacy della Guardia di Finanza.

COME OTTEMPERARE ALLE DISPOSIZIONI DI LEGGE

Come abbiamo descritto, il nuovo codice sulla privacy prevede una serie piuttosto complessa di misure da adottare e non si limita a suggerimenti generali, ma prevede precisi adeguamenti tecnici e organizzativi.

Non sempre all'interno dell'organizzazione aziendale vi sono le competenze tecniche e organizzative adeguate per portare a termine questa delicata missione.

La nostra esperienza diretta in numerose aziende ed enti pubblici, oltre che le notizie che ogni giorno ci giungono, confermano che spesso molti dei provvedimenti organizzativi e tecnologici necessari non sono stati adottati o non sono stati implementati correttamente, con il risultato che molte aziende non possono ritenersi tranquille né nei confronti dei controlli che il Garante e la Guardia di Finanza stanno effettuando in tutto il territorio nazionale, né nei confronti delle minacce alla sicurezza che, con l'espandersi dell'utilizzo di strumenti informatici e con la tendenza ad ampliare i collegamenti alla rete Internet, aumentano considerevolmente.

Data Security si propone, quindi, come vostro referente per tutte le esigenze della vostra struttura legate a sicurezza e privacy, allegando a questo scopo una breve descrizione della propria attività.

Approfondimenti e dettagli sono inoltre disponibili al sito Web <http://www.datasecurity.it>

Profilo di Data Security

Data Security è una società specializzata nella gestione della sicurezza e della privacy, in grado di fornire servizi che vanno dall'analisi dei rischi fino all'implementazione e integrazione di sofisticate soluzioni tecnologiche.

Ciò che distingue in maniera significativa Data Security è la capacità di padroneggiare e integrare le componenti organizzative, normative, tecnologiche e di processo per realizzare soluzioni realmente efficaci e in sintonia con l'organizzazione e i sistemi, a costi ragionevolmente contenuti.

Di seguito si riportano i servizi tipicamente erogati da Data Security:

- analisi dei rischi e valutazione delle priorità di intervento;
- analisi costi/benefici e studi di affidabilità tecnologica e prestazionale;
- installazione e configurazione di soluzioni per il monitoraggio e la gestione degli accessi ad Internet;
- consulenza legale, tecnica e organizzativa su Sicurezza, Privacy, Autenticazione, Firma Digitale e Business Continuità;
- collaudo e certificazione dei sistemi e delle procedure di Sicurezza;
- formazione qualificata agli incaricati e ai responsabili del trattamento dei dati, sia presso le strutture didattiche di Data Security sia presso la sede del cliente;
- test di vulnerabilità dei sistemi informatici dall'esterno e dall'interno della rete;
- definizione di regolamenti e policy per la sicurezza e il corretto utilizzo delle risorse informatiche e telematiche;
- consulenza dedicata alla Pubblica Amministrazione per la redazione e l'aggiornamento del Documento Programmatico sulla Sicurezza (D.Lgs. 196/2003), per lo sviluppo del sistema di gestione della sicurezza (Direttiva Interministeriale del 16/01/02) e per l'implementazione di Firma Digitale, della Carta del Cittadino e della Carta di identità elettronica;
- progettazione di sistemi di Storage, Disaster Recovery e Business Continuity.

Tutto questo con una costante attenzione al rapporto costi/benefici delle soluzioni proposte.

Oltre a ciò Data Security è in grado di fornire, attraverso i suoi partner, le migliori soluzioni tecnologiche per la Sicurezza informatica e di integrarle con i sistemi esistenti. Data Security si avvale della partnership tecnologica delle più importanti società mondiali nel settore della sicurezza informatica.

