La tutela dei dati personali tra DPS e modelli organizzativi

a cura dell'Avvocato Marco Maglio

LUCERNA IURIS – LEGAL EUROPEAN NETWORK
AVVOCATO MARCO MAGLIO

Introduzione

Che cosa è la protezione dei dati personali? E cosa vuol dire proteggere la riservatezza delle informazioni che trattiamo nella nostra attività?

Tutti sappiamo che esiste, ormai da diverso tempo, quella che viene comunemente chiamata "legge sulla privacy", ma pochi di noi sono davvero informati sugli effetti pratici di questa normativa.

Questa presentazione intende fornire una guida operativa di facile applicazione a vantaggio di tutti coloro che per motivi professionali devono svolgere attività di trattamento dei dati.

Obiettivo fondamentale è contribuire ad una effettiva diffusione della cultura della riservatezza in ambito professionale e per aiutare tutti alla soluzioni di questioni collegate alla prassi quotidiana ed alla redazione del Documento Programmatico sulla Sicurezza.

Introduzione

Obiettivo di questo scritto è dare un inquadramento generale sulle nozioni essenziali in materia di protezione dei dati personali, per poi affrontare i contenuti essenziali del Documento Programmatico sulla Sicurezza, la più importante tra le misure minime per garantire la protezione dei dati personali.

Completano il quadro di orientamento generale alcuni riferimenti bibliografici e la presentazione di una specifica sezione dedicata ai temi della tutela della riservatezza.

In particolare segnaliamo che tra le misure minime di sicurezza il "Codice in materia di protezione dei dati personali" prevede a carico dei Titolari del trattamento l'obbligo di predisporre specifici piani di formazione a favore degli incaricati al trattamento.

Questa presentazione è anche uno strumento introduttivo che può aiutare a gestire questo adempimento.

Cosa è la privacy

La privacy, intesa come diritto ad essere lasciati soli, è un diritto fondamentale oggi riconosciuto dall'ordinamento giuridico di tutti i paesi europei e delle principali nazioni del mondo.

Fin dalla sua origine la privacy è stata intesa come uno strumento per proteggere la propria riservatezza e difendersi dai comportamenti invadenti di chi intendeva violare tale aspettativa al segreto.

La privacy può essere considerata lo strumento attraverso il quale ognuno può definire un confine tra sé e gli altri. Si tratta di una situazione giuridica che disciplina il modo in cui una persona si relaziona con gli altri.

Cosa è la privacy

Per tale motivo il concetto stesso di privacy e il suo significato hanno subito nel tempo profondi cambiamenti, in relazione al mutare della società e degli **strumenti tecnologici** utilizzati, che non hanno però modificato un concetto fondamentale: ogni persona resta titolare del diritto di disporre dei dati che la descrivono e che ne qualificano l'individualità.

L'attuale legislazione in materia di dati personali, deriva dall'evoluzione che nel tempo ha interessato il concetto di privacy, quindi, per capire il reale significato di queste regole, è importante comprendere che la tutela della privacy oggi si occupa principalmente di garantire **il diritto fondamentale di esercitare il pieno e consapevole controllo sui nostri dati personali**.

Quando si parla di privacy, quindi, oggi non si fa riferimento solo al diritto alla riservatezza, ma anche al nostro **diritto di scelta** circa l'uso che vogliamo gli altri facciano dei nostri dati personali.

Cosa sono i dati personali

Per poter comprendere le regole a protezione della privacy occorre chiarire cosa si intende per

“dato personale”.

Tale aspetto è infatti essenziale per comprendere le regole ed applicarle correttamente.

Secondo la normativa, il dato personale è **qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.**

Dato personale è però anche **un'immagine, un suono e qualunque notizia o informazione che sia riferibile a un soggetto determinato o determinabile.**

Cosa sono i dati personali

I codici identificativi, sia quelli ricavati da dati anagrafici (ad esempio il codice fiscale), che i codici univoci attribuiti a una persona in base a criteri predefiniti (ad esempio i codici cliente) sono dati personali.

Dato personale è quindi **qualsiasi informazione riferita** (**o** anche semplicemente **riferibile** tramite un codice) **a una persona**: anche il numero di targa di una vettura riferita a un proprietario o il numero di una polizza riferita a un assicurato.

Cosa sono i dati personali

Una categoria particolare di dati personali sono i

dati sensibili.

Si tratta dei 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**.

Questa tipologia di dati è sottoposta a un livello di protezione più elevato di quello previsto per i dati non sensibili.

Proteggere i dati personali: principi generali

Consideriamo ora su quali capisaldi si basa la legislazione per proteggere le informazioni ed **evitare abusi** che violino la riservatezza delle persone cui si riferiscono quei dati.

Malgrado le norme che proteggono i dati personali siano molto complesse ed articolate, è possibile individuare alcuni principi fondamentali ai quali le regole si ispirano: è necessario conoscere questi principi per comprendere quali criteri garantiscono la protezione dei dati personali.

In coerenza con questi principi fondamentali infatti, la normativa fissa esplicitamente alcune **regole** molto precise circa le modalità del trattamento e i requisiti dei dati.

I principi fondamentali ricavati dalla lettura della normativa e dai provvedimenti delle autorità sono:

Proteggere i dati personali: principi generali

1. Diritto alla protezione dei dati personali

Si tratta della regola fondamentale (non a caso formulata in apertura del Codice in materia di dati personali, dall'articolo 1 del D. Lgs. 196/03) che attribuisce ad ogni individuo il diritto di pretendere che l'uso dei suoi dati personali si svolga nel rispetto dei suoi diritti e libertà fondamentali, nonché della sua dignità, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

A tal fine il trattamento dei dati personali è disciplinato assicurando un elevato livello di tutela dei diritti e delle libertà nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati, nonché per l'adempimento degli obblighi da parte dei titolari del trattamento.

Proteggere i dati personali: principi generali

2. Principio di necessità nel trattamento dei dati

È il criterio che mira a limitare le raccolte ed i trattamenti di dati non necessari.

A questo scopo la normativa (art. 3 del D. Lgs. 196/03) impone di configurare i sistemi informativi e i programmi informatici riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi o attraverso opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

In pratica si introduce un criterio di limitazione nella raccolta dei dati. Vanno raccolti solo i dati necessari per il trattamento che si intende realizzare.

Proteggere i dati personali: principi generali

3. Principio di finalità

È il principio che collega l'attività di raccolta dei dati personali con l'uso che di quelle informazioni viene fatto.

In pratica questo principio consiste nell'obbligo posto a carico di chi effettua la raccolta di far conoscere all'interessato – all'atto della raccolta – la ragione per la quale i dati sono raccolti: questa finalità deve essere legittima, determinata e non incompatibile con l'impiego dei dati.

Proteggere i dati personali: principi generali

4. Principio di autodeterminazione informativa

Questa regola fissa il principio per il quale ognuno di noi ha il diritto di determinare l'ambito di comunicazione dei dati che lo riguardano.

Quindi ogni individuo ha diritto di stabilire se ed in che misura le informazioni a lui riferite possono circolare ed essere conosciute dagli altri.

Proteggere i dati personali: principi generali

5. Principio di correttezza

È un principio che riguarda la condotta di chi usa i dati personali: questo soggetto deve comportarsi garantendo la liceità e la correttezza del trattamento, tanto durante la raccolta quanto durante l'elaborazione vera e propria dei dati.

Il trattamento è **lecito** quando è conforme alla legge, mentre è **corretto** quando la raccolta di dati avviene presso l'interessato in modo trasparente e non mediante ricorso ad artifizi e raggiri.

Proteggere i dati personali: principi generali

6. Principio di precauzione

Nell'utilizzo dei dati personali occorre prevenire ogni forma di illecito utilizzo di trattamento di dati personali, anche per mera negligenza o imperizia.

Pertanto chi tratta dati personali deve adottare qualsiasi cautela per evitare l'accesso a dati di provenienza non definita e di cui non sia possibile ricostruire le modalità di formazione.

In coerenza con questi principi fondamentali la normativa fissa esplicitamente alcune regole molto precise circa le modalità del trattamento ed i requisiti dei dati.

Proteggere i dati personali: principi generali

Rispettare i principi che abbiamo ora esaminato è importante

perché

i dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.

Quindi, rispettare questi principi permette di prevenire contestazioni che possono portare al blocco del trattamento dei dati (che significa non poter più svolgere la propria attività).

Trattamento dei dati personali: informativa e consenso

Esaminiamo ora il meccanismo sul quale si basa la protezione dei dati a partire dall'analisi del trattamento dei dati stessi.

Per "trattamento" si intende qualunque **operazione o complesso di operazioni**, effettuati anche senza l'ausilio di strumenti elettronici, **concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati**, anche se non registrati in una banca di dati.

Come si può ben intendere dalla semplice lettura della descrizione normativa, pressoché qualsiasi operazione compiuta nei confronti dei dati personali costituisce "**trattamento**".

Trattamento dei dati personali: informativa e consenso

La normativa disciplina anche i dati posti su supporti cartacei. Per tale motivo il concetto di trattamento comprende anche le operazioni che prescindono dall'utilizzo di **strumenti elettronici**.

La regola che disciplina il trattamento dei dati è semplice: ognuno ha **diritto di essere informato** che qualcun altro sta raccogliendo informazioni sul suo conto ed intende trattarle**;** ha diritto di sapere per quali **finalità** e con quali **modalità** tali dati sono raccolti e deve sapere quali diritti può esercitare su quel trattamento**.**

Dopo aver ricevuto queste informazioni la persona cui si riferiscono i dati ha **diritto di decidere** se consentire o non consentire quel trattamento**.**

Trattamento dei dati personali: informativa e consenso

La procedura di protezione dei dati personali è tutta racchiusa in questo meccanismo: chi intende trattare i dati ha **l'obbligo di informare** la persona cui si riferiscono i dati. Questa, sulla base delle informazioni ricevute ha diritto di scegliere se permettere o vietare questo trattamento**.**

Da un lato è posto l'obbligo di informare l'interessato oralmente o per iscritto, e dall'altro è stabilito **l'obbligo di chiedere il consenso** espresso all'interessato per poter effettuare l'operazione di trattamento (salvi i casi in cui il consenso non è necessario).

Va infine ricordato che la regola generale di trattamento basata su informativa e consenso conosce alcune importanti **eccezioni.** Infatti mentre l'informativa va sempre fornita all'interessato, la normativa prevede alcuni **casi in cui il consenso non è richiesto.**

Trattamento dei dati personali: informativa e consenso

Infine occorre tenere presente che il trattamento di dati personali effettuato da persone fisiche **per fini esclusivamente personali** è soggetto all'applicazione del presente codice solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione.

Per quanto riguarda i **limiti territoriali di applicabilità** di queste regole va ricordato che la normativa sul trattamento dei dati personali disciplina il trattamento di dati personali, anche detenuti all'estero, effettuato da chiunque è stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello Stato.

Soggetti del trattamento dei dati personali

Esaminiamo chi sono i soggetti che intervengono nelle operazioni di trattamento dei dati personali.

Le figure cui la normativa attribuisce poteri di controllo sono:

- il **titolare**
- il **responsabile**
- l'**incaricato**
- l'**interessato**
- il **Garante per la tutela dei dati personali**
- l'**Autorità Giudiziaria ordinaria**

Soggetti del trattamento dei dati personali

Per **titolare**, s'intende la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono anche unitariamente ad altro titolare, le decisioni in ordine alle **finalità** e alle **modalità** del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza. Quando il trattamento è effettuato da una persona giuridica o da un ente titolare è l'entità nel suo complesso e non la persona fisica che la rappresenta.

Il **responsabile** del trattamento è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo **preposto** al trattamento di dati personali. La sua nomina non è obbligatoria ma è lasciata alla discrezionalità del titolare. Il responsabile procede al trattamento attenendosi alle istruzioni impartite per iscritto dal titolare che, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle norme di legge e delle proprie istruzioni.

Soggetti del trattamento dei dati personali

Gli **incaricati** del trattamento sono le persone fisiche autorizzate a **compiere operazioni** di trattamento dal titolare o dal responsabile. Si tratta quindi dei soggetti che possono elaborare i dati personali, ai quali accedono attenendosi alle istruzioni ricevute dal titolare o dal responsabile.

L'**interessato** è il soggetto (persona fisica, persona giuridica, ente o associazione) **cui si riferiscono i dati personali**. È quindi il vero protagonista del trattamento.

L'autorità preposta alla tutela della riservatezza dei dati personali è il **Garante** per la protezione dei dati personali. Dal punto di vista generale il Garante è un'autorità amministrativa indipendente. Le **funzioni principali** del Garante sono controllare la legittimità dei trattamenti, esaminare i ricorsi e le segnalazioni ricevute dagli interessati.

Soggetti del trattamento dei dati personali

La normativa italiana fa inoltre esplicito riferimento alla giurisdizione del Giudice ordinario. Infatti resta ferma la possibilità di far valere i diritti fondamentali attribuiti all'interessato, oltre che con ricorso davanti al Garante, mediante l'esercizio dell'azione davanti all' Autorità Giudiziaria.

Tuttavia la tutela offerta dal Garante è alternativa a quella fornita dal **Giudice Ordinario**: il ricorso al Garante non può essere proposto se, per il medesimo oggetto e tra le stesse parti, è stata già adita l'Autorità Giudiziaria.

Compete sempre alla magistratura ordinaria ogni azione volta ad ottenere il risarcimento del danno tanto patrimoniale quanto non patrimoniale.

Sanzioni in caso di violazione delle regole

La normativa, in caso di violazione delle regole che disciplinano il trattamento dei dati, prevede alcune sanzioni che possono essere applicate dal Garante o dall'Autorità Giudiziaria ordinaria.

Le **sanzioni** possono essere:

- **penali:** comportano l'applicazione di pene detentive o pecuniarie da parte dell'Autorità Giudiziaria;

- **amministrative:** determinano l'applicazione di sanzioni pecuniarie da parte del Garante o di specifiche limitazioni rispetto al libero trattamento dei dati personali; in particolare il Garante può disporre il blocco del trattamento dei dati.

Sanzioni in caso di violazione delle regole

L'interessato che ritiene di aver subito un danno dall'illegittimo trattamento dei dati può chiedere, esclusivamente all'Autorità Giudiziaria, il risarcimento del danno subito.

La normativa prevede una particolare ipotesi di responsabilità extracontrattuale per i danni cagionati a seguito di trattamento di dati personali.

Infatti in questi casi si applica la disciplina prevista dal codice civile per l'esercizio di attività pericolose, in base alla quale, per evitare di essere obbligati al risarcimento occorre dimostrare di aver adottato tutte le misure idonee a evitare il danno.

Sanzioni in caso di violazione delle regole

La normativa prevede inoltre espressamente che, in caso di **violazione della disciplina in materia di modalità del trattamento e requisiti dei dati**, è risarcibile anche il danno non patrimoniale, cioè il danno che non incide direttamente sull'integrità economica dell'interessato.

Si tratta di quello che viene comunemente definito **danno non patrimoniale.**

Peraltro, rimane in ogni caso a carico del danneggiato l'onere di provare l'esistenza del nesso causale fra l'attività di trattamento dei dati personali e l'evento dannoso.

10 regole da ricordare

Cerchiamo ora di **tradurre in pratica** le regole che disciplinano la materia della privacy, individuando alcuni "comportamenti virtuosi", basati sull'esperienza e sull'**applicazione concreta** delle regole giuridiche.

L'adozione di questi criteri di comportamento agevola nell'individuazione di un metodo per evitare condotte a rischio e per escludere gli abusi nell'utilizzo dei dati personali.

Ecco **dieci regole** da ricordare per **trattare correttamente i dati personali** nell'ambito di un'organizzazione complessa.

10 regole da ricordare

1

Custodire in modo riservato banche dati, contratti e comunque ogni documentazione raccolta nello svolgimento dell'attività lavorativa.

10 regole da ricordare

2

Adottare cautele organizzative per garantire che tutte le persone con cui si collabora siano informate sulle regole di riservatezza adottate per proteggere i dati ed impartire adeguate istruzioni per evitare abusi per negligenza, imprudenza o imperizia.

10 regole da ricordare

3

Verificare sempre l’origine dei dati utilizzati.

10 regole da ricordare

4

In caso di utilizzo dei dati ricordarsi di verificare che se persona che si contatta abbia fornito il consenso e accertarsi se sia necessario disporne per utilizzare corettamente i dati.

10 regole da ricordare

5

Informare prontamente la persona preposta al trattamento dei dati qualora un interessato formuli un'istanza per l'esercizio dei suoi diritti.

10 regole da ricordare

6

Evitare di utilizzare liste di nominativi ed indirizzi quando non ne è certa la provenienza o il fornitore si è rifiutato di dichiarare per iscritto che l'uso dei dati è consentito ai sensi della vigente normativa, esonerando da qualsiasi conseguenza derivante da tale uso.

10 regole da ricordare

7

Adottare tutte le misure di sicurezza informatiche previste dal sistema fornito dall'organizzazione in cui si opera, quando ci si connette alla rete predisposta per il collegamento alla banca dati.

10 regole da ricordare

8

Segnalare al proprio referente qualsiasi anomalia riscontrata nella qualità dei dati presenti nel data base utilizzato.

10 regole da ricordare

9

Adottare ogni precauzione nello svolgimento di attività che prevedono l'utilizzo di dati personali (invio di materiale per posta, e-mail o ricerche di mercato con strumenti di telemarketing), al fine di prevenire ogni forma, anche per mera negligenza o imperizia, di illecito utilizzo di dati personali.

10 regole da ricordare

10

Ferma restando la responsabilità del singolo utilizzatore del data base, attenersi alle istruzioni che sono state e che verranno impartite dallo Studio per garantire la corretta gestione dei dati stessi.

Tutela dei dati e misure di sicurezza

Le regole giuridiche da sole non sono sufficienti per garantire l'effettiva tutela dei diritti degli interessati.

Oltre ad ulteriori regole legate all'autodisciplina dei singoli titolari dei trattamenti, occorre utilizzare procedure di sicurezza e strumenti tecnologici che permettano di **prevenire** ogni illegittimo trattamento di dati personali.

Per questo motivo è importante che all'interno di un'organizzazione siano adottate misure di sicurezza sia di tipo organizzativo che di tipo fisico e informatico per **evitare** possibili abusi nei trattamenti dei dati personali**.**

Il Codice in materia di protezione dei dati personali prevede l'adozione di misure di sicurezza **di diversa natura** a seconda che il trattamento dei dati avvenga con o senza l'ausilio di strumenti elettronici.

Tutela dei dati e misure di sicurezza

Trattamento di dati personali per tramite di strumenti elettronici

È consentito agli incaricati dotati di **credenziali di autenticazione** (user-id e password).

La parola chiave deve essere di almeno 8 caratteri, ovvero di un numero pari al massimo consentito, e **va modificata ogni 6 mesi** (**3** nel caso di trattamento di **dati sensibili o giudiziari**).

Devono essere fornite istruzioni scritte agli incaricati affinché l'accesso ai dati sia limitato in funzione dell'attività concretamente svolta.

Tutela dei dati e misure di sicurezza

Dovranno, inoltre, esser fornite istruzioni per la custodia di copie di sicurezza tramite salvataggio dei dati con frequenza almeno settimanale (cosiddetto *back up* dei dati).

È previsto l'utilizzo di strumenti elettronici di protezione (antivirus e firewall) da aggiornare con scadenza almeno semestrale.

La normativa dedica particolare attenzione al **documento programmatico sulla sicurezza** atto a fornire idonee informazioni riguardo alla sicurezza.

Ne parleremo in dettaglio tra poco.

Tutela dei dati e misure di sicurezza

Trattamento dei dati senza l'ausilio di mezzi informatici

Vanno impartite agli incaricati **istruzioni scritte** circa il controllo e la custodia di atti e documenti.

Va redatto un elenco degli incaricati individuandone i profili di autorizzazione; l'accesso agli archivi deve essere controllato e le persone ammesse dopo l'orario devono essere identificate e registrate.

Se il titolare omette l'adozione delle misure minime è prevista la **pena dell'arresto sino a due anni** o, alternativamente, l'**ammenda da euro 10.000 a 50.000**.

Il Documento Programmatico sulla Sicurezza

Che cos'è il Documento Programmatico sulla Sicurezza?

Il Documento Programmatico è una delle misure minime di Sicurezza che, in un quadro di evoluzione tecnologica costante, va aggiornato almeno una volta all'anno da parte del Titolare, anche avvalendosi dei responsabili eventualmente designati.

È un **documento interno** che va conservato agli atti e **non va inviato** a nessuna autorità di controllo.

Non è necessario che il documento abbia data certa. La legge non lo richiede.

È importante che il documento sia realizzato descrivendo correttamente la realtà e che si dia notizia dell'avvenuta redazione nella relazione che accompagna il Bilancio.

Il Documento Programmatico sulla Sicurezza

Quando va redatto il DPS?

Il documento programmatico va aggiornato entro il **31 marzo** di ogni anno.

Nel caso in cui il titolare ometta l'adozione delle misure minime è prevista la **pena dell'arresto sino a due anni** o, alternativamente, l'**ammenda da euro 10.000 a 50.000**.

Il Documento Programmatico sulla Sicurezza

Qual è il contenuto del DPS?

Il DPS deve fornire idonee informazioni riguardo a :

- l'elenco dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità in relazione al trattamento dei dati;
- l'analisi dei rischi;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché le disposizioni per la protezione dei locali destinati alla custodia;

Il Documento Programmatico sulla Sicurezza

- 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 a favore degli incaricati del trattamento;

- 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;

- l'individuazione dei criteri da adottare per la cifratura o per la separazione dei dati relativi alla salute ed alla vita sessuale dagli altri dati personali dell'interessato. (Questo punto riguarda peraltro quasi esclusivamente gli organismi sanitari e gli esercenti professioni sanitarie).

Come si redige il DPS

Il primo elemento da tenere presente nella redazione del DPS è il fatto che si tratta di uno strumento che definisce un **programma** per garantire la sicurezza e gestire correttamente i rischi.

Si tratta in pratica di predisporre un progetto, relativo alla sicurezza e descrittivo di tre aspetti essenziali:

- la situazione attuale
- i rischi attuali e potenziali
- gli strumenti e le precauzioni adottate per gestire questi rischi

Come si redige il DPS

Per redigere il documento programmatico occorre raccogliere alcune informazioni di base che permettano di formulare correttamente l'analisi dei rischi e definire gli strumenti di prevenzione più adeguati.

Lo strumento più semplice per raccogliere queste informazioni è rispondere ad alcuni specifici quesiti che ci permettono di analizzare punto per punto i requisiti tecnici di un sistema informatico sotto tre profili:

- strumenti di autenticazione informatica
- sistemi di autorizzazione
- altre misure di sicurezza

Vediamo i quesiti relativi a questi tre aspetti distintamente.

Come si redige il DPS

Strumenti di autenticazione informatica

1. Gli utenti sono dotati delle credenziali di autenticazione che consentano il proprio login al sistema?
1.1. Il login al sistema consente all'utente di accedere indistintamente a tutte le informazioni presenti sul sistema informatico? In caso di risposta affermativa passare al punto 2.
1.2. In caso si disponga di accessi personalizzati, l'ambito di utilizzo delle risorse per ciascun utente è stato definito e/o comunicato per iscritto all'utente?
2. Le credenziali di autenticazione sono composte da user name e da password? In caso di risposta negativa passare al punto 2.3.
2.1. Gli utenti dispongono di parole chiave univoche, a loro solamente riservate e da loro solamente conosciute?
2.2. Gli utenti possono scambiarsi user name e password tra loro?
2.3. Le credenziali di autenticazione sono state sostituite da altri sistemi (esempio: il riconoscimento biometrico dell'incaricato con codice identificativo o password)?

Come si redige il DPS

Strumenti di autenticazione informatica

3. Le credenziali di autenticazione sono univocamente assegnate o associate individualmente ad un solo utente?
4. Sono state impartite per iscritto agli incaricati le raccomandazioni di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato?
5. Le password sono composte da almeno otto caratteri?
5.1. Nel caso in cui lo strumento elettronico non lo permetta, le password sono composte da un numero di caratteri pari al massimo consentito?
5.2. Gli utenti sono stati interdetti dall'utilizzo di codici identificativi agevolmente riconducibili all'incaricato?
5.3. Gli utenti sono stati interdetti dall'utilizzo di codici identificativi contenenti riferimenti di tipo personale, come la data di nascita o il nome dell'animale domestico?

Come si redige il DPS

Strumenti di autenticazione informatica

5.4. Le password sono state modificate dopo il primo utilizzo?
5.5. Le password sono cambiate almeno ogni sei mesi (tre in presenza di dati sensibili)?
6. Sono state adottate regole per il non utilizzo da parte di altri incaricati di codici di identificazione, già attribuiti ad altri soggetti, anche in tempi diversi?
7. È prevista la disattivazione delle credenziali di autenticazione non utilizzate da almeno sei mesi?
7.1. Sono previste speciali autorizzazioni per le credenziali eventualmente utilizzate per soli scopi di gestione tecnica?
8. È prevista la procedura per disabilitare le credenziali di autenticazione in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali?
9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento?

Come si redige il DPS

Strumenti di autenticazione informatica

10. Nei casi di impedimento e/o prolungata assenza dell'incaricato, oppure di indispensabile e indifferibile intervento per necessità di operatività e di sicurezza del sistema sono state impartite idonee e preventive disposizioni scritte per individuare le modalità con le quali il titolare può disporre dei dati e degli strumenti elettronici?

10.1. Esiste una copia delle credenziali di autenticazione?

10.2. Le copie delle credenziali sono state affidate per iscritto ad un custode/responsabile?

10.3. I responsabili della custodia delle password sono stati avvisati con istruzione scritta del loro dovere di informare tempestivamente l'incaricato degli eventuali interventi effettuati?

11. Gli incaricati al trattamento sono stati informati che le disposizioni sul sistema di autenticazione (di cui ai punti precedenti) e quelle sul sistema di autorizzazione non sono applicabili ai trattamenti dei dati personali destinati alla diffusione?

Come si redige il DPS

Sistemi di autorizzazione

12. Il sistema di autorizzazione, atto a verificare le credenziali, discrimina gli ambiti di autorizzazioni in base ai profili di autorizzazione prestabiliti?
13. 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?
14. È stato adottato un piano delle verifiche periodiche (almeno annuali) per la verifica della sussistenza delle condizioni per la conservazione dei profili di autorizzazione?

Come si redige il DPS

Altre misure di sicurezza

15. Sono stati eseguiti raggruppamenti per classi omogenee di incarico?
15.1. L'accesso alla classe omogenea è regolamentato?
15.2. L'accesso alla classe omogenea è conforme al profilo di autorizzazione?
15.3. Classi omogenee e profili di autorizzazione vengono periodicamente sottoposti a verifica (almeno annuale)?
16. I dati personali sono protetti contro il rischio di intrusione (art. 615 – quinquies C.P.)?
16.1. Si dispone di antivirus aggiornato settimanalmente (anche se l'aggiornamento previsto per legge è semestrale)?
16.2. Si dispone di Firewall (software e/o hardware)?
16.3. Si dispone di connessione Internet con IP stabile?
16.4. Si dispone di rete Wireless?
16.5. Si dispone di protocollo di autenticazione Wireless?

Come si redige il DPS

Altre misure di sicurezza

17. I programmi per elaboratore che consentono di allontanare il rischio intrusione sono aggiornati almeno ogni dodici mesi (sei se si trattano dati sensibili)?
18. Le copie vengono eseguite ogni settimana?
18.1. Le copie sono depositate in cassaforte ignifuga?
18.2. Esiste un registro delle copie?
18.3. È stato definito un incaricato ed un apposito piano di ripristino da copia in caso di perdita totale o parziale dei dati?

Conclusioni

Dopo aver risposto a queste domande sarà più facile realizzare un DPS corrispondente alle esigenze della vostra struttura.

Per applicare correttamente queste regole occorre trovare il giusto equilibrio tra esigenze di sicurezza e semplicità organizzativa.

La ricerca di questo equilibrio richiede coraggio, spirito costruttivo e creatività per individuare i modelli organizzativi corretti.

Bibliografia

- Marco Maglio – *Le misure minime di sicurezza informatica: verso la redazione del documento programmatico di sicurezza* –PMI n. 4/2004
- Marco Maglio – *L'uso degli strumenti informatici da parte dei lavoratori alla ricerca dell'equilibrio tra diritto alla riservatezza e dovere di controllo* –PMI n. 5/2004
- Garante per la Protezione dei dati personali – *Prime riflessioni sui criteri di redazione del documento programmatico sulla sicurezza* – 13 maggio 2004
- Garante per la Protezione dei dati personali – *Guida operativa per redigere il Documento programmatico sulla sicurezza (DPS)* – 2004
- a cura di Juri Monducci Giovanni Sartor – *Il codice in materia di protezione dei dati personali: commentario sistematico al D.Lgs. 30 giugno 2003 n. 196* – CEDAM 2004
- a cura di Giuseppe Cassano e Stefano Fadda – *Codice in materia di protezione dei dati personali: commento articolo per articolo al testo unico sulla privacy D.Lgs. 30 giugno 2003. n. 196* – IPSOA 2004
- Francesco Cardarelli, Salvatore Sica e Vincenzo Zeno-Zencovich – *Il codice dei dati personali:Temi e Problemi* – Giuffrè Editore 2004.