Il Documento Programmatico Sulla Sicurezza

L'art. 34 del Codice prevede tra le misure minime l'adozione del c.d. Documento Programmatico sulla Sicurezza (DPS).

La stesura di un documento sulla sicurezza non è disposizione nuova, in quanto il precedente D.P.R. 318/1999 faceva pure riferimento all'obbligo di predisporre ed aggiornare, con cadenza annuale, un documento programmatico sulla sicurezza dei dati.

Al fine di disciplinare le misure di sicurezza, il precedente D.P.R. 318/1999 imponeva quest'obbligo a chiunque operasse il trattamento di dati sensibili e giudiziari mediante elaboratori elettronici accessibili in rete pubblica.

Oggi essendo venuta meno la distinzione tra elaboratori in rete accessibili al pubblico, o no, l'obbligo è previsto per tutti gli elaboratori (sia singolo, che in rete) che trattino dati personali di natura sensibile o giudiziaria, con esclusione delle ipotesi di semplificazione previste dal legislatore.

È comunque sempre consigliabile la stesura di un DPS anche in caso di trattamento di dati comuni con strumenti elettronici. Detta stesura risponde infatti a quei criteri di misure idonee (non minime) che mettono al riparo il titolare dalle responsabilità civili ex art. 2050 c.c., e – comunque - risponde all'osservanza di criteri di buona organizzazione aziendale.

Il DPS va redatto ogni 31 marzo ed ha il compito specifico di indurre a fare, almeno una volta all'anno, il punto sul sistema di sicurezza adottato e da adottare nell'ambito della propria attività; tale documento ha una funzione meramente descrittiva, eppure per la sua violazione il Codice prevede sanzioni estremamente severe, che vanno dall'arresto fino a due anni (e conseguente inevitabile sanzione disciplinare prevista dal Codice deontologico) al possibile pagamento di somme da 20.000 a 120.000 euro (rispettivamente art. 169 ed art. 162 co. 2-bis del Codice).

In effetti come si evince facilmente dal tenore dell'allegato B, nel DPS non deve essere riassunto l'intero assetto delle misure minime adottate e delle modalità specifiche con le quali queste vengono esplicate, ma pare essere sufficiente una ricognizione, seguendo punto per punto il citato art. 19 dell'allegato B.

Il Garante è intervenuto più volte per dare utili indicazioni in merito all'effettiva compilazione del DPS, prima il 13 maggio 2004 con delle prime riflessioni sui criteri di redazione del DPS e poi l'11 giugno 2004 con una vera e propria guida operativa per redigere il Documento programmatico sulla sicurezza.

Diciamo subito che non esiste e non può esistere un DPS modello che possa andare bene per tutte le realtà organizzative. Le associazioni professionali, gli enti, gli uffici legali ed anche i singoli si sono cimentati nella redazione di DPS anche particolareggiati validi per intere categorie di aziende o professionisti. Purtroppo nessuno è dotato, fino a prova contraria, di poteri paranormali per cui non può prevedere la struttura organizzativa di un'azienda nè le sue effettive misure di sicurezza. Di conseguenza anche il modello migliore necessita di quegli adattamenti indispensabili che possano conformare il DPS alla specifica realtà organizzativa. Saranno anche minimi adattamenti ma sono necessari per evitare di trovarsi in situazioni davvero imbarazzanti.

Per non parlare, poi, dei software che stanno girando in questo periodo sulla redazione dei DPS. Questo è il classico caso di "deriva tecnologica" di cui spesso parla l'Autorità Garante volendo indicare tutti quei casi in cui diventa davvero inutile se non addirittura svantaggioso ricorrere all'applicazione delle nuove tecnologie.

Sinceramente appare davvero impensabile che un software (tranne casi limite di intelligenza artificiale estremamente sofisticata) possa consentire la corretta redazione di un documento piuttosto complesso come il DPS.

Passando adesso alla parte pratica il DPS deve cercare di seguire punto per punto quanto previsto dall'art. 19 del disciplinare tecnico (allegato B al D.lgs.) e cioè:

1) Elenco dei trattamenti di dati personali (punto 19.1) mediante:

1.1) individuazione dei dati personali trattati

1.2) descrizione delle aree, dei locali e degli strumenti con i quali si effettuano i trattamenti

1.3) l'elaborazione della mappa dei trattamenti effettuati

2) Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati (punto 19.2)
3) Analisi dei rischi che incombono sui dati (punto 19.3)
4) Misure atte a garantire l'integrità e la disponibilità dei dati in essere e da adottare (punto 19.4)
5) Criteri e modalità di ripristino della disponibilità dei dati (punto 19.5)
6) Pianificazione degli interventi formativi previsti (punto 19.6)
7) Adozione misure minime di sicurezza in caso di trattamento di dati personali affidati all'esterno (punto 19.7)
8) Procedure per il controllo sullo stato della sicurezza
9) Dichiarazioni d'impegno e firma

Solo eventuale (specialmente per le strutture sanitarie) è quanto prevista dal punto 19.8 e cioè la cifratura dei dati o separazione dei dati identificativi.

*Elenco dei trattamenti di dati personali (regola 19.1***)**

Riguardo il primo punto e cioè l'elenco dei trattamenti dei dati personali si tratta di indicare innanzitutto la tipologia dei dati trattati descrivendo inoltre le aree, i locali e gli strumenti con i quali si effettuano i trattamenti.

In questa sede diventa molto importante descrivere l'organizzazione degli schedari e degli altri supporti cartacei nonchè indicare la presenza di elaboratori in rete oppure non in rete, descrivendone le caratteristiche, e di eventuali impianti di videosorveglianza.

In definitiva quindi per ciascun trattamento vanno indicate le seguenti informazioni:

- Descrizione sintetica: menzionare il trattamento dei dati personali attraverso l'indicazione della finalità perseguita o dell'attività svolta (es., fornitura di beni o servizi, gestione del personale, ecc.) e delle categorie di persone cui i dati si riferiscono (clienti o utenti, dipendenti e/o collaboratori, fornitori, ecc.).
- Natura dei dati trattati: indicare se, tra i dati personali, sono presenti dati sensibili o giudiziari.
- Struttura di riferimento: indicare la struttura (ufficio, funzione, ecc.) all'interno della quale viene effettuato il trattamento. In caso di strutture complesse, è possibile indicare la macro-struttura (direzione, dipartimento o servizio del personale), oppure gli uffici specifici all'interno della stessa (ufficio contratti, sviluppo risorse, controversie sindacali, amministrazione-contabilità.).
- Altre strutture che concorrono al trattamento: nel caso in cui un trattamento, per essere completato, comporta l'attività di diverse strutture è opportuno indicare, oltre quella che cura primariamente l'attività, le altre principali strutture che concorrono al trattamento anche dall'esterno.
- Descrizione degli strumenti elettronici utilizzati: va indicata la tipologia di strumenti elettronici impiegati (elaboratori o p.c. anche portatili, collegati o meno in una rete locale, geografica o Internet; sistemi informativi più complessi).

Ulteriori elementi potrebbero essere:

- Identificativo del trattamento: alla descrizione del trattamento, se ritenuto utile, può essere associato un codice, facoltativo, per favorire un'identificazione univoca e più rapida di ciascun trattamento nella compilazione delle altre tabelle.
- Banca dati: indicare eventualmente la banca dati (ovvero il data base o l'archivio

informatico), con le relative applicazioni, in cui sono contenuti i dati. Uno stesso trattamento può richiedere l'utilizzo di dati che risiedono in più di una banca dati. In tal caso le banche dati potranno essere elencate.

- Luogo di custodia dei supporti di memorizzazione: indicare il luogo in cui risiedono fisicamente i dati, ovvero dove si trovano (in quale sede, centrale o periferica, o presso quale fornitore di servizi, ecc.) gli elaboratori sui cui dischi sono memorizzati i dati, i luoghi di conservazione dei supporti magnetici utilizzati per le copie di sicurezza (nastri, CD, ecc.) ed ogni altro supporto rimovibile.
- Tipologia di dispositivi di accesso: elenco e descrizione sintetica degli strumenti utilizzati dagli incaricati per effettuare il trattamento: pc, terminale non intelligente, palmare, telefonino, ecc.
- Tipologia di interconnessione: descrizione sintetica e qualitativa della rete che collega i dispositivi d'accesso ai dati utilizzati dagli incaricati: rete locale, geografica, Internet, ecc.

Appare opportuno redigere a livello dimostrativo una mappa dei trattamenti che sintetizza a livello grafico quanto descritto in precedenza.

Distribuzione dei compiti e delle responsabilità (regola 19.2)

In questa sede va indicato innanzitutto il titolare del trattamento dei dati con relative generalità ed incarico.

Vanno indicati anche gli eventuali soggetti incaricati sintetizzando le istruzioni che vengono fornite agli stessi e che costituiscono l'oggetto della lettera di incarico.

In particolare oltre alle istruzioni generali su come devono essere trattati i dati personali, agli incaricati sono fornite esplicite istruzioni relativamente a:

- procedure da seguire per la classificazione dei dati personali, al fine di distinguere quelli sensibili e giudiziari, osservando le maggiori cautele di trattamento che questo tipo di dati richiedono;
- modalità di reperimento dei documenti contenenti dati personali e modalità da osservare per la custodia e l'archiviazione degli stessi;
- modalità per elaborare e custodire le password necessarie per accedere agli elaboratori elettronici e ai dati in essi contenuti, nonchè per fornirne copia al preposto alla custodia della parola chiave;
- prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici, mentre è in corso una sessione di lavoro;

- procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi;
- procedure per il salvataggio dei dati;
- modalità di utilizzo, custodia e archiviazione dei supporti rimuovibili contenenti dati personali;
- aggiornamento continuo, utilizzando il materiale e gli strumenti forniti dal Titolare, sulle misure di sicurezza.

Analisi dei rischi che incombono sui dati (regola 19.3)

Questa è la parte più delicata di un DPS e richiede una certa attenzione.

Una buona impostazione potrebbe essere quella di tener conto di due tipi di rilevazioni:

- la tipologia dei dati trattati, la loro appetibilità, nonché la loro pericolosità per la privacy dei soggetti cui essi si riferiscono;
- i comportamenti degli operatori, gli eventi relativi agli strumenti utilizzati per il trattamento dei dati, gli eventi relativi al contesto.

Riguardo il primo aspetto l'analisi dei rischi con la valutazione dell'incidenza di rischio dovrebbe avere come riferimento:

i dati comuni del personale dipendente (quali quelli necessari al rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi, ai rapporti fiscali), i dati comuni dei clienti (compresi i dati sul patrimonio e sulla situazione economica, o necessari per disposizioni fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi), i dati comuni di terzi (compresi i dati sul patrimonio e sulla situazione economica, o necessari per disposizioni fiscali o afferenti alla corrispondenza con gli stessi), i dati comuni dei fornitori (concernenti la corrispondenza con gli stessi, nonché inerenti ai rapporti fiscali) ed i dati comuni dei clienti, dei fornitori o di terzi ricavati da albi, elenchi pubblici, visure camerali.

I dati sensibili del personale dipendente, i dati sensibili dei clienti dagli stessi forniti, i dati sensibili di terzi.

Riguardo il secondo aspetto l'analisi può essere semplificata attraverso la redazione di distinte tabelle che tengano conto del comportamento degli operatori, degli eventi relativi agli strumenti e degli eventi relativi al contesto.

Le tabelle potrebbero essere di questo tipo:

COMPORTAMENTO DEGLI OPERATORI

Rischi	Si/No	gravità
Sottrazione di credenziali di autenticazione		
Carenza di consapevolezza, disattenzione o incuria		
Comportamenti sleali o fraudolenti		
Errore materiale		
Altro evento		

EVENTI RELATIVI AGLI STRUMENTI

Rischi	Si/No	gravità
Azione di virus informatici o di programmi suscettibili di recare danno		
Spamming o tecniche di sabotaggio		
Malfunzionamento, indisponibilità o degrado degli strumenti		
Accessi esterni non autorizzati		
Intercettazioni di informazioni in rete		
Altro evento		

EVENTI RELATIVI AL CONTESTO

Rischi	Si/No	gravità
Accessi non autorizzati a locali/aree ad accesso ristretto		
Sottrazione di strumenti contenenti dati		
Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, ecc.) nonchè dolosi, accidentali o dovuti ad incuria		
Guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.)		
Errori umani nella gestione della sicurezza fisica		
Altro evento		

È possibile, per ulteriori dettagli, rinviare a documenti analoghi già redatti in tema di piani di sicurezza e gestione del rischio, come ad es.: Business Continuity Plan, Disaster Recovery Plan, ecc. (si tenga però presente che le analisi alla base di questi altri documenti possono avere una natura ben diversa).

Molte aziende, ad esempio, predispongono per la loro attività un piano di disaster recovery che passa attraverso diverse fasi.

Innanzitutto è necessario fare un elenco dei potenziali disastri che potrebbero verificarsi sulla rete. Tra le cause principali si segnalano il malfunzionamento dei dischi, l'interruzione temporanea delle operazioni, i virus, gli attacchi di hackers, la distruzione fisica.

Il passo successivo nella creazione del piano consiste nel definire le priorità per applicazioni automatizzate, nel senso che devono essere determinate le funzioni del sistema che devono essere ripristinate immediatamente dopo un disastro e quelle che invece possono aspettare. Nella stesura di questa parte del processo di pianificazione i risultati migliori si ottengono quanto più onestamente i dipendenti ammettano la importanza delle loro funzioni per l'azienda ovvero quanto più agevolmente tale valutazione possa essere compiuta sulla base di criteri oggettivi. In ogni caso il lavoro

da compiere risulta difficoltoso poiché è necessario predisporre una catalogazione di tutte le applicazioni, operazione non sempre agevole. Normalmente si distingue tra *funzioni essenziali per attività a tempo pieno* (si tratta di operazioni che devono proseguire in modo continuativo per il buon andamento dell'azienda), *funzioni vitali a tempo parziale* (si tratta di operazioni che devono continuare ma che hanno luogo periodicamente in specifici momenti), *funzioni necessarie per obiettivi aziendali di secondaria importanza* (sono operazioni considerate necessarie ma non rappresentano obiettivi primari), *attività operative di routine*, *attività di crescita*.

Il terzo passo nella creazione del piano di Disaster Recovery consiste nell'identificare e implementare misure preventive. Sebbene il piano serva prevalentemente per decidere come comportarsi in caso di disastro, questo certamente non preclude la possibilità di prendere in esame modalità per prevenire i problemi o alleggerirne le conseguenze. D'altra parte la conoscenza e l'implementazione delle misure di protezione dei dati sono fondamentali per l'eventuale ripristino dopo il disastro. In particolare bisogna prendere in considerazione le seguenti precauzioni: il backup dei dati, la ridondanza dei dati, il software anti-virus, l'energia elettrica (gruppi di continuità), i firewall (sistemi di sicurezza contro possibili intrusioni di hackers), un centro dati alternativo.

Il passo successivo nel processo di pianificazione consiste nello scrivere le istruzioni di ripristino, preparare, cioè, un elenco dettagliato che spieghi esattamente che cosa fare quando un sistema qualsiasi deve essere ripristinato. Nel piano è necessario indicare le seguenti informazioni: persone da contattare per ciascun reparto; modalità per recuperare i nastri di backup e copie di altri media; nomi e informazioni sui fornitori che possano fornire immediatamente nuovi computer adeguati alle esigenze dell'utente; nomi e informazioni sui fornitori che possono offrire consulenti in grado di eseguire le operazioni di ripristino istruzioni per recuperare i dati dai supporti di backup; notizie dettagliate su come configurare le workstation e i server da utilizzare in una LAN ripristinata.

Infine è necessario perfezionare il piano, accertando altresì che il medesimo funzioni attraverso tests di verifica e sottoponendolo a revisione periodica.

Misure in essere e da adottare (regola 19.4)

Per misure bisogna intendere lo specifico intervento tecnico od organizzativo posto in essere (per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia), come pure quelle attività di verifica e controllo nel tempo, essenziali per assicurarne l'efficacia.

Le misure indicate devono garantire:

- la protezione delle aree e dei locali ove si svolge il trattamento dei dati personali;
- la corretta archiviazione e custodia di atti, documenti e supporti contenenti dati personali;
- la sicurezza logica, nell'ambito degli strumenti elettronici

Le successive misure indicate a sostegno della fase di protezione dei dati si suddividono in:

- misure già adottate al momento della stesura del presente documento;
- ulteriori misure finalizzate ad incrementare il livello di sicurezza nel trattamento dei dati.

Va indicata, innanzitutto la protezione delle aree e dei locali (dispositivi antincendio, impianti di condizionamento, adeguamento legge 46/90, ecc.). Inoltre vanno indicate tutte le cautele per regolamentare l'accesso nei locali archivio ed impedire l'ingresso di estranei.

Va anche in questo caso ricordato che agli incaricati vengono impartite istruzioni per la gestione, la custodia e l'archiviazione dei documenti e dei supporti.

Una particolare attenzione va dedicata alle c.d. misure logiche di sicurezza per il trattamento effettuato con strumenti elettronici.

In particolare si fa riferimento:

- alla realizzazione e gestione di un sistema di autenticazione informatica al fine di accertare l'identità delle persone che hanno accesso agli strumenti elettronici; in particolare ciascun utilizzatore deve essere dotato di una password di almeno 8 caratteri (o minore per le caratteristiche del sistema). Detta password non contiene, nè conterrà, elementi facilmente ricollegabili all'organizzazione o alla persona del suo utilizzatore, né allo studio legale. La stessa viene autonomamente scelta dall'utilizzatore e dallo stesso custodita in una busta chiusa che viene consegnata al responsabile del trattamento, il quale provvede a depositarla in un contenitore chiuso a chiave in un plico sigillato. Ogni tre mesi ciascun incaricato provvede a sostituire la propria password. Le password dovranno essere automaticamente disattivate dopo tre mesi di non utilizzo;
- all' autorizzazione e definizione delle tipologie di dati ai quali gli incaricati posso accedere e utilizzare al fine delle proprie mansioni lavorative;
- alla protezione di strumenti e dati da malfunzionamenti e attacchi informatici;
- alla prescrizione delle opportune cautele per la custodia e l'utilizzo dei supporti

rimovibili, contenenti dati personali.

Naturalmente bisogna indicare l'esistenza di programmi antivirus e di sistemi firewall anti-intrusione e l'eventuale esistenza di supporti rimovibili che contengano dati personali.

Criteri e modalità di ripristino della disponibilità dei dati (regola 19.5)

In questa sede vanno descritti i criteri e le procedure adottati per il ripristino dei dati in caso di loro danneggiamento o di inaffidabilità della base dati. L'importanza di queste attività deriva dall' eccezionalità delle situazioni in cui il ripristino ha luogo: è essenziale che, quando sono necessarie, le copie dei dati siano disponibili e che le procedure di reinstallazione siano efficaci.

Pertanto, è opportuno descrivere sinteticamente anche i criteri e le procedure adottate per il salvataggio dei dati al fine di una corretta esecuzione del loro ripristino.

Bisogna innanzitutto indicare la banca-dati interessata, i criteri e procedure per il salvataggio dei dati (descrivendo sinteticamente la tipologia di salvataggio e la frequenza con cui viene effettuato), le modalità di custodia delle copie (indicando il luogo fisico in cui sono custodite le copie dei dati salvate), la struttura o persona incaricata del salvataggio.

Pianificazione degli interventi formativi previsti (regola 19.6)

In questa sezione bisogna innanzitutto descrivere sinteticamente gli obiettivi e le modalità degli interventi formativi in relazione a quanto previsto dalla regola 19.6 (ingresso in servizio o cambiamento di mansioni degli incaricati, introduzione di nuovi elaboratori, programmi o sistemi informatici, ecc) .

Inoltre bisogna individuare le classi omogenee di incarico a cui l'intervento è destinato e/o le tipologie di incaricati interessati, anche in riferimento alle strutture di appartenenza.

È opportuno indicare anche i tempi previsti per lo svolgimento degli interventi formativi.

Trattamenti affidati all'esterno (regola 19.7)

Qualora determinate attività che comportino trattamento di dati siano affidate a terzi è necessario redigere un quadro sintetico di tali attività con l'indicazione sintetica del quadro giuridico o contrattuale (nonché organizzativo e tecnico) in cui tale

trasferimento si inserisce, in riferimento agli impegni assunti, anche all'esterno, per garantire la protezione dei dati stessi.
In particolare va indicata l'attività affidata all'esterno; i trattamenti di dati, sensibili o giudiziari, effettuati nell'ambito della predetta attività; la società, l'ente o il consulente cui è stata affidata l'attività, e il ruolo ricoperto agli effetti della disciplina sulla protezione dei dati personali (titolare o responsabile del trattamento).
Inoltre vanno descritti gli oneri a cui è sottoposta la società esterna affinché sia garantito un adeguato trattamento dei dati: ad esempio può essere ritenuto necessario che la società a cui viene affidato il trattamento rilasci specifiche dichiarazioni o documenti, oppure assuma alcuni impegni anche su base contrattuale, con particolare riferimento, a: trattamento di dati ai soli fini dell'espletamento dell'incarico ricevuto; adempimento degli obblighi previsti dal Codice per la protezione dei dati personali; rispetto delle istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o integrazione delle procedure già in essere; impegno a relazionare periodicamente sulle misure di sicurezza adottate –anche mediante eventuali questionari e liste di controllo- e ad informare immediatamente il titolare del trattamento in caso di situazioni anomale o di emergenze.

Cifratura dei dati o separazione dei dati identificativi (regola 19.8)

Questo punto riguarda solo organismi sanitari e esercenti professioni sanitarie.
In questo caso vanno rappresentate le modalità di protezione adottate in relazione ai dati per cui è richiesta la cifratura -o la separazione fra dati identificativi e dati sensibili-, nonché i criteri e le modalità con cui viene assicurata la sicurezza di tali trattamenti.
In particolare è opportuno descrivere i trattamenti (le banche o le basi di) dati oggetto della protezione; riportare la tipologia di protezione adottata, scelta fra quelle indicate dal Codice o in base a considerazioni specifiche del titolare; descrivere sinteticamente, in termini tecnici ed eventualmente organizzativi, la misura adottata.
Ad esempio, in caso di utilizzo di cifratura, le modalità di conservazione delle chiavi e le procedure di utilizzo.
La dichiarazione d'impegno e di firma conclude il DPS e si ricorda che affinché la data apposta sia certa è opportuna o l'apposizione di un timbro anche da parte dell'Ufficio postale oppure la semplice spedizione del Documento a se stessi.

Una volta redatto il DPS deve essere custodito presso la sede della società, per essere esibito in caso di controllo. Sarebbe utile anche indicare con apposito avviso da affiggere in uno spazio visibile l'avvenuta redazione del DPS.
Infine è buona norma allegare al DPS l'organigramma dei soggetti responsabili in tema di privacy e la lettera di incarico da distribuire agli incaricati.

Modello base

Documento Programmatico sulla Sicurezza

Redatto ai sensi e per gli effetti dell'articolo 34, comma 1, lettera g) del D.Lgs. 196/2003 e del disciplinare tecnico (allegato B del D.Lgs. n. 196/2003)

SCOPO

Scopo di questo documento è di delineare il quadro delle misure di sicurezza, organizzative, fisiche e logiche, da adottare per il trattamento dei dati personali effettuato dalla …….

In particolare nel Documento Programmatico Sulla Sicurezza vengono definiti i criteri tecnici e organizzativi per:

a. la protezione delle aree e dei locali interessati dalle misure di sicurezza, nonché le procedure per controllare l'accesso delle persone autorizzate ai medesimi locali;
b. i criteri e le procedure per assicurare l'integrità dei dati;
c. i criteri e le procedure per la sicurezza della trasmissione dei dati, ivi compresi quelli per le redazioni di accesso per via telematica;
d. l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni.

In conformità con quanto prescritto al punto 19 del Disciplinare tecnico (allegato B al D.Lgs.) nel presente documento si forniscono idonee informazioni riguardanti:

10)Elenco dei trattamenti di dati personali (punto 19.1) mediante:

1.1) individuazione dei dati personali trattati

1.2) descrizione delle aree, dei locali e degli strumenti con i quali si effettuano i trattamenti

1.3) l'elaborazione della mappa dei trattamenti effettuati

11) Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati (punto 19.2)

12) Analisi dei rischi che incombono sui dati (punto 19.3)

13) Misure atte a garantire l'integrità e la disponibilità dei dati in essere e da adottare (punto 19.4)

14) Criteri e modalità di ripristino della disponibilità dei dati (punto 19.5)

15) Pianificazione degli interventi formativi previsti (punto 19.6)

16) Adozione misure minime di sicurezza in caso di trattamento di dati personali affidati all'esterno (punto 19.7)

17) Procedure per il controllo sullo stato della sicurezza

18) Dichiarazioni d'impegno e firma

1. ELENCO DEI TRATTAMENTI DI DATI PERSONALI

1.1 Tipologie di dati trattati.

Il Documento Programmatico Sulla Sicurezza riguarda tutti i dati personali:

- Sensibili
- Giudiziari
- Comuni

Il Documento Programmatico Sulla Sicurezza si applica al trattamento di tutti i dati personali per mezzo di:

- Strumenti elettronici di elaborazione
- Altri strumenti di elaborazione (es. cartacei, audio, visivi e audiovisivi, ecc.)

La ……..esercita un'attività di……..

La società tratta i seguenti dati:

dati comuni dei clienti, dei fornitori o di terzi ricavati da albi, elenchi pubblici, visure camerali; dati comuni del personale dipendente, quali quelli necessari al rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi o richiesti ai fini fiscali e previdenziali o dati di natura bancaria; dati comuni dei clienti, dagli stessi forniti per ragioni inerenti l'attività di vendita o di assistenza, compresi i dati sul patrimonio e sulla situazione economica, o necessari per fini fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi; dati comuni di terzi, forniti dai clienti compresi i dati sul patrimonio e sulla situazione economica, o necessari a fini fiscali; dati comuni dei fornitori concernenti la corrispondenza con gli stessi, nonché inerenti ai fini fiscali o dati di natura bancaria.

I dati non pubblici vengono acquisiti previa l'informativa che si allega al presente D.P.S.

1.2 Aree, locali e strumenti con i quali si effettuano i trattamenti

Il trattamento dei dati avviene nella sede e luogo di lavoro, situata in ……

Gli uffici (locale unico diviso in n…….. aree: una destinata alla ……., una ad ……., una a…….. ecc.) sono dislocati al piano…….. .

L'accesso agli stessi è controllato attraverso suoneria d'ingresso ed è protetto da impianto di allarme collegato alla centrale di P.S. (si/no)

A. Schedari ed altri supporti cartacei

I supporti cartacei sono raccolti in armadietti a loro volta custoditi come segue:

- Archivio 1 localizzato nell'area vendita composto da n….. armadietti ove vengono archiviati i supporti cartacei di comune e continuo utilizzo (preventivi, contratti, fatture);
- Archivio 2 localizzato nell'area ufficio composto da n…….. armadietti ove vengono archiviati i supporti cartacei di comune e continuo utilizzo (preventivi, contratti, fatture);
- Archivio 3 localizzato nell'area ufficio composto da n……. armadietto dotato di chiusura ove vengono archiviati i supporti cartacei contenenti dati di maggiore riservatezza inerenti la solvibilità economica della clientela.
- ……..

I supporti cartacei sono costituiti da contenitori chiusi di cartone rigido.

Agli archivi posso accedere solo le persone autorizzate.

B. Elaboratori non in rete

Non sono presenti.

C - Elaboratori in rete

Si dispone di una rete, realizzata mediante collegamenti Ethernet via cavo (o wireless) costituita da:

- n…….. postazioni lavoro così dislocate: una nell'area …….., una nell'area ……., una nell'area ……, ecc.
- n. …. stampante dislocata nell'area ……..
- n. fax - fotocopiatrice localizzato nell'area …….

Descrizione tecnica dei computer e programmi installati su di essi.

Principalmente descrizione dei software antivirus e firewall installati.

D – Impianti di videosorveglianza

Sono/Non sono utilizzati impianti di video-sorveglianza.

Analisi dei trattamenti effettuati

Dalla rilevazione degli strumenti utilizzati e delle tipologie di dati trattati emerge che:

1. solo i dati personali vengono trattati sistematicamente con supporti cartacei e con elaborazione;
2. gli eventuali dati sensibili trattati con elaborazione, sono limitati a quelli necessari per assolvere agli obblighi normativi e contrattuali;
3. gli eventuali dati giudiziari trattati anche con elaborazione sono quelli necessari per assolvere agli obblighi normativi e di Legge.

1.3 Mappa dei trattamenti effettuati

Dal riepilogo dei dati trattati e dall'identificazione degli strumenti utilizzati si delinea il seguente schema:

Tipologia trattamento	**Cartaceo**	**PC non in rete**	**PC in rete**	**Videosorveglianza**
Dati comuni relativi a clienti				
Dati comuni relativi ad altri soggetti				
Dati biometrici relativi a clienti				
Dati idonei a rilevare la posizione di ..				
Dati di natura giudiziaria				
Dati relativi al personale				
Dati sensibili relativi a clienti				
Dati idonei a rilevare lo stato di salute				

2. DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ

Titolare del trattamento dei dati

Per il trattamento dei dati personali il titolare è la …… che ha nominato come responsabile l'amministratore unico sig. …….che assume l'incarico di progettare, realizzare e mantenere in efficienza le misure di sicurezza.

Soggetti incaricati

Il trattamento dei dati personali viene effettuato solo da soggetti che hanno ricevuto un formale incarico mediante designazione per iscritto di ogni singolo incaricato, con il quale si individua l'ambito del trattamento consentito.

Gli incaricati sono il sig. ed il sig.

Le lettere di incarico che vanno a completare il mansionario sono allegate al presente documento (allegato B).

Istruzioni specifiche fornite ai soggetti incaricati

Oltre alle istruzioni generali su come devono essere trattati i dati personali, agli incaricati sono fornite esplicite istruzioni relativamente a:

- procedure da seguire per la classificazione dei dati personali, al fine di distinguere quelli sensibili e giudiziari, osservando le maggiori cautele di trattamento che questo tipo di dati richiedono;
- modalità di reperimento dei documenti contenenti dati personali e modalità da osservare per la custodia e l'archiviazione degli stessi;
- modalità per elaborare e custodire le password necessarie per accedere agli elaboratori elettronici e ai dati in essi contenuti, nonché per fornirne copia al preposto alla custodia della parola chiave;
- prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici, mentre è in corso una sessione di lavoro;
- procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi;

- procedure per il salvataggio dei dati;
- modalità di utilizzo, custodia e archiviazione dei supporti rimuovibili contenenti dati personali;
- aggiornamento continuo, utilizzando il materiale e gli strumenti forniti dal Titolare, sulle misure di sicurezza.

I dati comuni dei clienti, dei fornitori o di terzi sono trattati, oltre che dal responsabile del trattamento, anche da tutti gli incaricati.

I dati comuni del personale dipendente, i dati sensibili (eventuali) del personale dipendente, i dati afferenti i pagamenti a favore di terzi fornitori, la contabilità e i rapporti bancari dello studio sono esclusivamente tenuti dal responsabile.

3. ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

L'analisi dei possibili rischi che gravano sui dati è stata effettuata tenendo conto di due tipi di rilevazioni:

- la tipologia dei dati trattati, la loro appetibilità, nonché la loro pericolosità per la privacy dei soggetti cui essi si riferiscono;
- i comportamenti degli operatori, gli eventi relativi agli strumenti utilizzati per il trattamento dei dati, gli eventi relativi al contesto.

Riguardo il primo aspetto l'analisi dei rischi si può così sintetizzare:

per i dati comuni del personale dipendente (quali quelli necessari al rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi, ai rapporti fiscali), i dati comuni dei clienti (compresi i dati sul patrimonio e sulla situazione economica, o necessari per disposizioni fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi), i dati comuni di terzi (compresi i dati sul patrimonio e sulla situazione economica, o necessari per disposizioni fiscali o afferenti alla corrispondenza con gli stessi), i dati comuni dei fornitori

(concernenti la corrispondenza con gli stessi, nonché inerenti ai rapporti fiscali) ed i dati comuni dei clienti, dei fornitori o di terzi ricavati da albi, elenchi pubblici, visure camerali: il rischio legato alla loro gestione può definirsi basso/ medio.

Per (gli eventuali) dati sensibili del personale dipendente, (eventuali) dati sensibili dei clienti dagli stessi forniti; (eventuali) dati sensibili di terzi il rischio legato alla loro gestione è da definirsi medio.

Riguardo il secondo aspetto sono state elaborate le seguenti tabelle:

COMPORTAMENTO DEGLI OPERATORI

Rischi	**Si/No**	**gravità**
Sottrazione di credenziali di autenticazione		
Carenza di consapevolezza, disattenzione o incuria		
Comportamenti sleali o fraudolenti		
Errore materiale		
Altro evento		

EVENTI RELATIVI AGLI STRUMENTI

Rischi	**Si/No**	**gravità**
Azione di virus informatici o di programmi suscettibili di recare danno		
Spamming o tecniche di sabotaggio		
Malfunzionamento, indisponibilità o degrado degli strumenti		
Accessi esterni non autorizzati		
Intercettazioni di informazioni in rete		
Altro evento		

EVENTI RELATIVI AL CONTESTO

Rischi	Si/No	gravità
Accessi non autorizzati a locali/aree ad accesso ristretto		
Sottrazione di strumenti contenenti dati		
Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, ecc.) nonché dolosi, accidentali o dovuti ad incuria		
Guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.)		
Errori umani nella gestione della sicurezza fisica		
Altro evento		

4. MISURE ATTE A GARANTIRE L'INTEGRITÀ E LA DISPONIBILITÀ DEI DATI IN ESSERE E DA ADOTTARE.

Alla luce dei fattori di rischio e delle aree individuate nel precedente paragrafo vengono descritte le misure atte a garantire:

- la protezione delle aree e dei locali ove si svolge il trattamento dei dati personali;

- la corretta archiviazione e custodia di atti, documenti e supporti contenenti dati personali;
- la sicurezza logica, nell'ambito degli strumenti elettronici

Le successive misure indicate a sostegno della fase di protezione dei dati si suddividono in:

- misure già adottate al momento della stesura del presente documento;
- ulteriori misure finalizzate ad incrementare il livello di sicurezza nel trattamento dei dati.

4.1 La protezione di aree e locali

Per quanto concerne il rischio che i dati vengano danneggiati o perduti a seguito di eventi distruttivi, per quanto lo stesso sia stato valutato basso, le aree ove si svolge il trattamento dei dati sono protette da:

- dispositivi antincendio previsti dalla normativa vigente (legge 626/94) (si/no)
- impianto di condizionamento (si/no)
- adeguamento legge 46/90 (si/no)

Sono adottate le seguenti misure per impedire accessi non autorizzati:

Il locale ove si svolge l'attività della società è protetto da impianto di allarme collegato con la centrale di P.S. Lo stesso è soggetto a vigilanza notturna. (si/ no).

L'archivio contenente dati di maggiore riservatezza dovrà essere chiuso a chiave. Gli incaricati devono comunque controllare l'accesso agli archivi. Fuori dall'orario di lavoro l'accesso agli archivi è consentito previa registrazione.

Si è data istruzione che il materiale cartaceo asportato e destinato allo smaltimento dei rifiuti sia riposto negli appositi sacchi di plastica e che detti

sacchi siano chiusi in modo che atti e documenti negli stessi contenuti non possano accidentalmente fuoriuscire, e che detto materiale sia giornalmente asportato.

4.2 Custodia e archiviazione dei dati

Agli incaricati sono state impartite istruzioni per la gestione, la custodia e l'archiviazione dei documenti e dei supporti. In particolare sono state fornite direttive per:

- il corretto accesso ai dati personali, sensibili e giudiziari;
- la conservazione e la custodia di documenti, atti e supporti contenenti dati personali, sensibili e giuridici;
- la definizione delle persone autorizzate ad accedere ai locali archivio e le modalità di accesso;
- non lasciare incustoditi sulle scrivanie, o su altri ripiani, atti, documenti e fascicoli delle pratiche. I fascicoli vanno conservati negli appositi schedari e prelevati per il tempo necessario al trattamento per esservi poi riposti;
- assicurare che le comunicazioni a mezzo posta, o a mezzo telefax, siano tempestivamente smistate e consegnate ai destinatari.

4.3 Misure logiche di sicurezza

Per il trattamento effettuato con strumenti elettronici si sono individuate le seguenti misure:

- realizzazione e gestione di un sistema di autenticazione informatica al fine di accertare l'identità delle persone che hanno accesso agli strumenti elettronici; in particolare ciascun utilizzatore deve essere dotato di una password di almeno 8 caratteri (o minore per le caratteristiche del sistema).

Detta password non contiene, né conterrà, elementi facilmente ricollegabili all'organizzazione o alla persona del suo utilizzatore, né allo studio legale. La stessa viene autonomamente scelta dall'utilizzatore e dallo stesso custodita in una busta chiusa che viene consegnata al responsabile del trattamento, il quale provvede a depositarla in un contenitore chiuso a chiave in un plico sigillato. Ogni tre mesi ciascun incaricato provvede a sostituire la propria password. Le password dovranno essere automaticamente disattivate dopo tre mesi di non utilizzo;

- autorizzazione e definizione delle tipologie di dati ai quali gli incaricati posso accedere e utilizzare al fine delle proprie mansioni lavorative;
- protezione di strumenti e dati da malfunzionamenti e attacchi informatici;
- prescrizione delle opportune cautele per la custodia e l'utilizzo dei supporti rimovibili, contenenti dati personali.

Accesso ai dati e istruzioni impartite agli incaricati

Gli incaricati al trattamento dei dati, dovranno osservare le seguenti istruzioni per l'utilizzo degli strumenti informatici:

- obbligo di custodire i dispositivi di accesso agli strumenti informatici (username e password);
- obbligo di non lasciare incustodito e accessibile lo strumento elettronico assegnato durante una sessione di trattamento;
- obbligo di assoluta riservatezza;
- divieto di divulgazione della password di accesso al sistema.

Protezione di strumenti e dati

Premesso che non vengono trattati dati sensibili e giudiziari in rete, il sistema di elaborazione è comunque protetto da programmi antivirus e di sistema

firewall anti-intrusione. Il sistema è altresì impostato per l'aggiornamento periodico automatico di protezione.

Agli incaricati è stato affidato il compito di controllare, almeno ogni tre mesi, l'aggiornamento automatico.

Supporti rimovibili

Gli stessi non contengono dati personali.

5. CRITERI E MODALITÀ DI RIPRISTINO DELLA DISPONIBILITÀ DEI DATI

Per i dati trattati con strumenti elettronici sono previste procedure di backup attraverso le quali viene periodicamente effettuata una copia di tutti i dati presenti nel sistema. Il salvataggio dei dati avviene:

- con frequenza mensile
- le copie vengono custodite in un luogo protetto

Custode di detti backup è stato nominato il responsabile del trattamento.

L'operazione viene svolta tramite disco fisso rimovibile per cui ogni backup si sovrappone al precedente.

6. PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI PREVISTI

Agli incaricati al trattamento, il responsabile del trattamento fornisce la necessaria formazione:

- al momento dell'ingresso in servizio
- in occasione di cambiamenti di mansione
- in occasione dell'introduzioni di nuovi strumenti e programmi informatici

La formazione ad ogni modo deve avere una frequenza annuale. Essa tende a sensibilizzare gli incaricati sulle tematiche di sicurezza, facendo comprendere i

rischi e le responsabilità (con specificazione delle sanzioni connesse penali e disciplinari) che riguardano il trattamento dei dati personali.

Inoltre, essa tende alla compiuta spiegazione del concetto di quale sia la natura ed il contenuto dei dati sensibili e giudiziari, con l'invito a segnalare eventuali disfunzioni dei sistemi operativi e, nel dubbio, di richiedere al titolare se un dato possa avere o meno natura sensibile o giudiziaria.

7. TRATTAMENTI AFFIDATI ALL'ESTERNO

Nello svolgimento dell'attività vengono/ non vengono affidati dati personali all'esterno.

Se si specificare quale attività viene svolta all'esterno e chi la svolge.

8. CONTROLLO GENERALE SULLO STATO DELLA SICUREZZA

Il responsabile mantiene aggiornate le misure di sicurezza al fine di adottare gli strumenti più idonei per la tutela dei dati trattati. Egli verifica inoltre con frequenza almeno mensile l'efficacia delle misure adottate relativamente a:

- accesso fisico a locali dove si svolge il trattamento
- procedure di archiviazione e custodia dati trattati
- efficacia e utilizzo misure di sicurezza strumenti elettronici
- integrità dei dati e delle loro copie di backup
- distruzione dei supporti magnetici non più riutilizzabili
- livello di informazione degli interessati

9. DICHIARAZIONE D'IMPEGNO E FIRMA

Il presente documento redatto in data …… viene firmato in calce dal sig. ……..in qualità di amministratore unico della ……e verrà aggiornato periodicamente entro il 31 marzo di ogni anno.

L'originale del presente documento è custodito presso la sede della società, per essere esibito in caso di controllo.

Data e luogo

Firma dell'Amministratore unico

_____

Allegato A

Organigramma privacy

TITOLARE DEI DATI

……..

RESPONSABILE

…….

INCARICATI AL TRATTAMENTO

…….

Allegato B

NOMINA DI INCARICATO DEL TRATTAMENTO DEI DATI

Il sottoscritto _____ [*indicare il nominativo/denominazione del titolare o del responsabile*], *con sede legale/residente* in [_____], Via [_____], in qualità di _____ [*Titolare/Responsabile]* del trattamento dei dati personali ai sensi del D.Lgs. 196/2003,

designa

il Sig. [_____] incaricato del trattamento dei dati personali necessari nell'ambito dello svolgimento della propria attività lavorativa.

Istruzioni specifiche sul trattamento dei dati

La informiamo che ai sensi dell'art. 11 del D.Lgs. 196/2003 i dati personali oggetto di trattamento devono essere:

- trattati in modo lecito e secondo correttezza;
- raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
- esatti e, se necessario, aggiornati;
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti e successivamente trattati;
- conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

A tale riguardo, si richiede la Sua particolare attenzione ai seguenti punti aventi specifica attinenza con la sicurezza dei dati trattati:

- procedure da seguire per la classificazione dei dati personali, al fine di distinguere quelli sensibili, osservando le maggiori cautele di trattamento che questo tipo di dati richiedono;
- modalità di reperimento dei documenti contenenti dati personali e modalità da osservare per la custodia e l'archiviazione degli stessi;
- modalità per elaborare e custodire le password necessarie per accedere agli elaboratori elettronici e ai dati in essi contenuti, nonché per fornire copia al preposto alla custodia della parola chiave;

- prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici, mentre è in corso una sessione di lavoro;
- procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi, nonché procedure per il salvataggio dei dati;
- modalità di utilizzo, custodia ed archiviazione dei supporti rimuovibili contenenti dati personali.

Modalità operative da osservare per il trattamento dei dati

Al fine della corretta gestione dei dati personali oggetto di trattamento, La invitiamo ad attenersi alle seguenti istruzioni:

- richiedere ed utilizzare solo i dati necessari alla normale attività lavorativa;
- non lasciare incustodito il proprio posto di lavoro prima di aver provveduto alla messa in sicurezza dei dati;
- limitare l'accesso ai dati all'espletamento delle proprie mansioni ed esclusivamente negli orari di lavoro;
- non lasciare incustoditi ed accessibili a terzi gli strumenti elettronici mentre è in corso una sessione di lavoro;
- comunicare e/o diffondere solo i dati personali preventivamente autorizzati dal Titolare e/o dal Responsabile;
- accertarsi che i terzi siano a conoscenza e abbiano autorizzato l'uso dei dati richiesti;
- accertarsi dell'identità di terzi e della loro autorizzazione al ritiro di documentazione in uscita;
- non fornire telefonicamente o a mezzo fax dati senza specifica autorizzazione e/o identificazione del richiedente;
- custodire e non divulgare il codice di identificazione personale (*username*) e la *password* di accesso agli strumenti elettronici;
- conservare e custodire la chiave di accesso all'archivio cartaceo con la massima cura e non lasciarla incustodita al fine di garantire che l'accesso all'archivio sia possibile solo ai soggetti autorizzati.

Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dovranno essere osservati anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro.

Qualsiasi altra informazione può esserLe fornita dal Titolare e/o dai Responsabili. Per ogni altra misura ed istruzione qui non prevista si rinvia al Documento Programmatico sulla Sicurezza.

La preghiamo di sottoscrivere la presente per presa visione di quanto riportato.

_____ [*luogo e data*]

Sig. _____ [*nome, cognome e firma dell'incaricato*]