Marzo

Studio di Consulenza Legale Aziendale e Tributaria
BATTAGLIONI

2010

SUPPLEMENTO

Speciale adempimenti Privacy 2010

Uno degli ambiti di forte impatto organizzativo e amministrativo per imprese e professionisti è senz'altro quello relativo alle disposizioni in tema di sicurezza nel trattamento dei dati, dal momento che il Codice della *Privacy* (D.Lgs. n.196/03) ha riscritto integralmente le disposizioni in tema di sicurezza.
L'art. 31 del D.Lgs. n.196/03 stabilisce che i dati personali devono essere "*custoditi e controllati … in modo da ridurre al minimo … i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta*".

Quando il trattamento, come nella grande maggioranza dei casi, avviene tramite **strumenti elettronici**,

▼

l'art.34 prevede espressamente, tra le misure di sicurezza, l'obbligo di redigere annualmente il "**documento programmatico sulla sicurezza**" **(entro il 31 marzo di ogni anno)**

▼

se si trattano dati sensibili o giudiziari, secondo lo *standard* illustrato nell'allegato B del Codice.

La platea dei soggetti interessati è ampissima e ancora oggi non tutte le realtà imprenditoriali ed economiche hanno integralmente adempiuto alle formalità prescritte dal D.Lgs. n.196/03. Considerando che il rispetto degli obblighi imposti dal Codice della *Privacy* porta alla redazione del DPS, **di seguito si propone un modello di Documento, allineato con le impostazioni proposte dall'Autorità Garante per la protezione dei dati personali, da integrare opportunamente, secondo le specifiche necessità**. Naturalmente, il *fac-simile* non ha la pretesa di essere esaustivo e risolutivo, costituendo la base per la sua redazione conforme alla realtà organizzativa e strutturale propria di ciascuna impresa / ciascun professionista per i quali si provvede a redigerlo.
Vengono, inoltre, allegate per completare lo "Speciale adempimenti *Privacy*" le seguenti carte di lavoro oltre ad uno scadenzario dei principali adempimenti:

- *Fac-simile* di informativa dati personali per dipendenti e collaboratori
- *Fac-simile* di lettera di nomina incaricati
- *Fac-simile* di lettera di nomina responsabili
- Istruzioni per la modifica e la custodia delle *password*
- Informativa da raccogliere presso clienti e fornitori

NOTE METODOLOGICHE
Nel documento di seguito proposto:

- le parti in **nero** sono quelle generalmente idonee per la totalità delle imprese interessate alla redazione del DPS;
- le parti in **blu** sono le sezioni che possono essere differenti, realtà per realtà;
- le parti in ***bordeaux*** e quelle su sfondo grigio sono le note operative, utili per la compilazione, ma da cancellare in sede di definizione del DPS.

Ai gentili Clienti

Loro sedi

Oggetto: NORMATIVA SULLA *PRIVACY* - ADOZIONE DELLE MISURE MINIME DI SICUREZZA

Il Codice sulla *Privacy* (D.Lgs. n.196/03) impone a tutti coloro che trattano dati personali la predisposizione di adeguati controlli in materia di sicurezza, sulla base di uno specifico protocollo previsto dal *c.d. Disciplinare Tecnico della norma* (allegato B del citato D.Lgs. n.196/03).
La norma obbliga alla realizzazione di diversi adempimenti, tra cui:

- la nomina del ***titolare del trattamento dei dati***, che generalmente coincide con la Società, nella persona del suo Legale rappresentante;
- la nomina del/dei ***responsabile/i del trattamento dei dati;***
- la nomina del/degli ***incaricato/i al trattamento dei dati;***
- il rilascio di apposita informativa,
- la preventiva richiesta del consenso al trattamento dei dati,
- la notificazione al Garante della *Privacy*, quando corra l'obbligo,
- l'**adozione di idonee misure di sicurezza**, per garantire che i dati personali vengano custoditi e controllati in modo da ridurre ad un ragionevole margine, il rischio di:
  - sottrazione, alterazione, perdita degli stessi,
  - di accesso non autorizzato da parte di terzi,
  - trattamento di dati non consentito e non conforme a quanto normativamente previsto.

È quanto mai opportuno ricordare che chi non adempie a quest'obbligo si espone al rischio di vedersi condannato, oltre che a pesanti sanzioni anche di natura penale, all'eventuale risarcimento dei danni che i terzi potrebbero lamentare come conseguenza dell'inefficiente controllo dell'attività di trattamento dei dati personali.
Il Legislatore, in relazione all'obbligo generale di protezione dei dati personali, ha previsto un livello minimo di sicurezza cui corrispondono le c.d. misure minime, tra le quali vi è anche la redazione del **DPS** (Documento Programmatico sulla Sicurezza) quando il trattamento dei dati viene effettuato con strumenti elettronici e riguarda dati "sensibili" (ossia idonei a rivelare l'origine etnica e razziale, le convinzioni religiose, politiche, filosofiche, l'appartenenza a partiti e sindacati, nonché quelli idonei a rivelare lo stato di salute e la vita sessuale), o "giudiziari".

Il DPS deve essere aggiornato e rivisto ogni anno entro il 31 marzo; periodicamente è necessario verificare il rispetto delle prescrizioni normative, e annualmente corre l'obbligo di effettuare un percorso formativo specifico da parte del titolare, dei responsabili e degli incaricati al trattamento dei dati.

Nel corso del 2008 sono state apportate importanti modifiche al Codice della *Privacy*, che hanno semplificato alcuni obblighi in materia di "misure minime di sicurezza" per determinate categorie di trattamento dei dati. In particolare:

con il provvedimento del Garante del 19/06/08	⇨ piccole e medie imprese, professionisti e artigiani possono godere di semplificazioni su alcuni adempimenti previsti dal D.Lgs. n.196/03, quali informativa, esonero dal consenso, incaricati del trattamento dei dati personali (come meglio specificato nel prosieguo);

con il D.L. n.112/08 (c.d. “Manovra estiva”)	⇨	sono state introdotte ulteriori semplificazioni in materia di DPS (dettagliate in altra informativa di questo speciale *Privacy*); in pratica ora è possibile **evitare** di redigere il documento programmatico sulla sicurezza **quando** i soggetti trattano soltanto dati non sensibili, ovvero, in presenza di dati sensibili, questi siano costituiti unicamente dallo stato di salute o malattia dei propri dipendenti e collaboratori a progetto, senza indicazione della relativa diagnosi o dall’adesione a organizzazioni sindacali o a carattere sindacale.

Qualora non vi abbiate già adempiuto, potete contattare il nostro Studio già dai prossimi giorni per quanto necessario.

firma

Ai gentili Clienti

Loro sedi

Oggetto: SEMPLIFICAZIONI *PRIVACY* PER LE PMI

La Manovra estiva del 2008 ha introdotto delle significative semplificazioni al Codice della *Privacy*. Esse riguardano, oltre al DPS di cui si dirà appena di seguito, anche la notificazione al Garante della *Privacy* e il trattamento dei dati personali fuori dalla UE. In particolare:

➲ La notificazione al Garante

Relativamente alla notificazione, che costituisce un obbligo solo al verificarsi di determinate e specifiche condizioni, ora la norma contiene un'esplicita indicazione delle informazioni che il titolare deve fornire attraverso il sito del Garante, utilizzando l'apposito modello.
Di seguito si ricordano le informazioni richieste dalla notificazione:

Le informazioni richieste nella notificazione
a) le coordinate identificative del titolare del trattamento e, eventualmente, del suo rappresentante, nonché le modalità per individuare il responsabile del trattamento, se designato;
b) la/le finalità del trattamento;
c) una descrizione della/delle categorie di persone interessate e dei dati o delle categorie di dati relativi alle medesime;
d) i destinatari o le categorie di destinatari a cui i dati possono essere comunicati;
e) i trasferimenti di dati previsti verso Paesi terzi;
f) una descrizione generale che permetta di valutare in via preliminare l'adeguatezza delle misure adottate per garantire la sicurezza del trattamento.

➲ Il trasferimento dei dati personali fuori dalla UE

Altra modifica, probabilmente quella meno rilevante per la gran parte dei soggetti interessati, riguarda il trasferimento di dati personali oggetto di trattamento verso un Paese non appartenente all'Unione europea. Tale trasferimento era consentito in precedenza solo se autorizzato dal Garante, sulla base di adeguate garanzie per i diritti dell'interessato, individuate e avallate dalla Commissione Europea o individuate dal Garante stesso anche in relazione a garanzie prestate contrattualmente. Ora il Garante potrà autorizzare il trasferimento dopo aver appurato l'esistenza delle necessarie garanzie, oltre che su base contrattuale, anche mediante regole di condotta esistenti nell'ambito di società appartenenti a un medesimo gruppo.

➲ Semplificazioni relative al DPS

a seguito delle modifiche introdotte dalla manovra estiva del 2008, il Documento Programmatico sulla Sicurezza (DPS), in molti casi ora è possibile che possa essere sostituito da una

"autocertificazione", e in molti degli altri casi è possibile che possa essere redatto in modo "semplificato" rispetto ai requisiti minimi.

Esonero dal DPS

In pratica ora è possibile **evitare** di redigere il documento programmatico sulla sicurezza **quando** i soggetti:

- trattano soltanto dati non sensibili;
- ovvero, in presenza di dati sensibili, questi siano costituiti unicamente:
  - dallo stato di salute o malattia dei propri dipendenti e collaboratori a progetto, senza indicazione della relativa diagnosi;
  - dall'adesione a organizzazioni sindacali o a carattere sindacale.

Si tratta molto spesso degli unici dati sensibili trattati da molte piccole o medie aziende, che, prima delle modifiche, costringevano alla redazione del DPS.
Per non redigere il DPS, sarà sufficiente che il titolare del trattamento dei dati renda un'autocertificazione (di cui all'art.47 del T.U. di cui al DPR n.445/00), in cui dichiari **di trattare soltanto tali dati in osservanza delle altre misure di sicurezza prescritte.**
Tali soggetti sono **esonerati** dalla nomina di una figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui sono effettuati trattamenti di dati personali (il c.d. "amministratore di sistema").

AUTOCERTIFICAZIONE SOSTITUTIVA DPS
Obbligo di cui alla lett.g) del co.1 e al punto 19 dell'Allegato B
Ai sensi degli artt.34 co.1-*bis* D.Lgs. n.196/03 e 47 DPR n.445/00

Il sottoscritto ……., nato a ……., in data …….., C.F. ……..……,
in qualità di Legale rappresentante società ……. con sede in ……..,
C.F. …….. P. Iva ……,
consapevole che il rilascio di false dichiarazioni ad un pubblico ufficiale o la presentazione di false documentazioni sono punibili a termine degli artt. 495 e 496 del Codice penale,

DICHIARA

Ai sensi dell'art.34, co.1-*bis* del D.Lgs. n.196/03

- ☐ di effettuare il trattamento di dati personali non sensibili;
- ☐ che gli unici dati sensibili trattati sono quelli costituiti dallo stato di salute o malattia dei propri dipendenti e collaboratori anche a progetto, senza indicazione della relativa diagnosi, ovvero dall'adesione ad organizzazioni sindacali o a carattere sindacale;
- ☐ che i dati di cui sopra sono trattati in osservanza delle misure di sicurezza prescritte dal D.Lgs. n.196/03 e dall'Allegato B) allo stesso.

……, lì…… Il Titolare del trattamento …….

DPS semplificato

Inoltre, secondo il testo del nuovo co.1-*bis,* art.34 del D.Lgs. n.196/03, in relazione ai trattamenti di cui sopra, nonché a quelli comunque effettuati per correnti finalità amministrative e contabili, in particolare presso piccole e medie imprese, liberi professionisti e artigiani, il Garante ha individuato con un primo provvedimento (27/11/08, in G.U. n.287/08), da aggiornare periodicamente, **modalità semplificate** di applicazione del disciplinare tecnico di cui all'allegato B), in ordine all'adozione delle **misure minime di sicurezza**.

In buona sostanza, si tratta di un'ulteriore semplificazione, legata più specificatamente alle misure minime di sicurezza, in ordine al trattamento di quei dati che possiamo definire "ordinari", come la tenuta di una contabilità piuttosto che la gestione di dati e documenti previsti per i datori di lavoro.
I soggetti interessati sono i titolari che:

- siano soggetti alla tenuta di un aggiornato DPS (quindi non nei casi di esonero);
- trattino dati personali "unicamente per correnti finalità amministrative e contabili" (il provvedimento parla, a titolo di esempio, di "gestione di ordinativi" e di "ordinaria corrispondenza con clienti, fornitori e dipendenti").

In particolare, tale agevolazione è rivolta alle seguenti categorie di **Titolari**:

piccoli imprenditori ai sensi dell'art. 2083 del Codice Civile	ovvero: "*i coltivatori diretti del fondo, gli artigiani, i piccoli commercianti e coloro che esercitano un'attività professionale organizzata prevalentemente con il lavoro proprio e dei componenti della famiglia*";
piccola e media impresa (PMI) ai sensi dell'art.2.1 del D.M. 18/04/05	"*Adeguamento alla disciplina comunitaria dei criteri di individuazione di piccole e medie imprese*" ovvero imprese che "*hanno meno di 250 occupati e un fatturato annuo non superiore a 50 milioni di euro, oppure un totale di bilancio annuo non superiore a 43 milioni di euro*".

Anche i predetti soggetti (come quelli che predispongono l'autocertificazione) sono esonerati dalla nomina dell'Amministratore di sistema.

DOCUMENTO PROGRAMMATICO "SEMPLIFICATO"

Imprese e professionisti ammessi al DPS semplificato:

- possono **impartire agli incaricati** le istruzioni in materia di **misure minime anche oralmente;**
- possono utilizzare per l'accesso ai sistemi informatici un qualsiasi sistema di **autenticazione basato su un *username* e una *password***; lo *username* deve essere disattivato quando viene meno il diritto di accesso ai dati (es. non si opera più all'interno dell'organizzazione);
- in caso di assenze prolungate o di impedimenti del dipendente possono mettere in atto procedure o modalità che consentano comunque l'operatività e la sicurezza del sistema (ad es. l'invio automatico delle mail ad un altro recapito accessibile);
- devono **aggiornare** i programmi di sicurezza (**antivirus) almeno una volta l'anno;**
- devono effettuare ***backup* dei dati almeno una volta al mese.**

A differenza del DPS ordinario, l'aggiornamento di quello semplificato è richiesto solo in presenza di modifiche.

Lo Studio rimane a disposizione per ogni ulteriore chiarimento.
Cordiali saluti.

firma

Ai gentili Clienti

Loro sedi

Oggetto: L'AMMINISTRATORE DI SISTEMA

Lo scorso 15 dicembre 2009 scadeva il termine per effettuare gli adempimenti previsti dalla disciplina della *Privacy* in materia di "amministratore di sistema", laddove evidentemente obbligatoria la sua istituzione. In particolare:

sono previsti i seguenti obblighi:

- individuare coloro che ricadono nella categoria di "amministratore di sistema";
- valutare l'esperienza, la capacità e l'affidabilità dei soggetti designati quali "amministratore di sistema" che devono fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza;
- designare tali "amministratore di sistema" in modo individuale con l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;
- verificare l'operato degli amministratori di sistema, con cadenza almeno annuale, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti;
- registrare gli accessi ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema, mediante l'adozione di sistemi idonei alla registrazione degli accessi logici (autenticazione informatica).

Possono essere considerati amministratori di sistema:

- gli amministratori di "basi di dati";
- gli "amministratori di reti" (es: titolare di Studio o dell'impresa che accede con la qualifica o le prerogative di "*administrator*" della rete) e di apparati di sicurezza;
- e gli "amministratori di sistemi *software* complessi" (es.: tecnico informatico nominato *ad hoc*), e ciò anche quando l'amministratore non consulti "in chiaro" le informazioni relative ai trattamenti di dati personali.

Gli "amministratori di sistema" sono figure essenziali per la sicurezza delle banche dati e la corretta gestione delle reti telematiche.

Sono esperti chiamati a svolgere delicate funzioni che comportano la concreta capacità di accedere a tutti i dati che transitano sulle reti aziendali ed istituzionali. Ad essi viene affidato spesso anche il compito di vigilare sul corretto utilizzo dei sistemi informatici di un'azienda o di una pubblica amministrazione.
Le ispezioni effettuate in questi anni dall'Autorità hanno permesso di mettere in luce in diversi casi una scarsa consapevolezza da parte di organizzazioni grandi e piccole del ruolo svolto dagli amministratori di sistema. I gravi casi verificatisi negli ultimi anni hanno evidenziato una preoccupante sottovalutazione dei rischi che possono derivare quando l'attività di questi esperti sia svolta senza il necessario controllo.

Le misure e le cautele da mettere in atto, tenendo presente che sono esclusi i trattamenti di dati, sia in ambito pubblico che privato, effettuati a fini amministrativo contabile, che pongono minori rischi per gli interessati, sono le seguenti:

Registrazione degli accessi	Adozione di sistemi di controllo che consentano la registrazione degli accessi effettuate dagli amministratori di sistema ai sistemi di elaborazione e agli archivi elettronici. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.
Verifica della attività	Verifica almeno annuale da parte dei titolari del trattamento sulla rispondenza dell'operato degli amministratori di sistema alle misure organizzative, tecniche e di sicurezza previste dalla legge per i trattamenti di dati personali.
Elenco degli amministratori di sistema e loro caratteristiche	Ciascuna azienda o soggetto pubblico dovrà inserire nel documento programmatico della sicurezza o in un documento interno (disponibile in caso di accertamenti da parte del Garante) gli estremi identificativi degli amministratori di sistema e l'elenco delle funzioni loro attribuite. Dovranno, infine, essere valutate con attenzione, esperienza, capacità, e affidabilità della persona chiamata a ricoprire il ruolo di amministratore di sistema, che deve essere in grado di garantire il pieno rispetto della normativa in materia di protezione dei dati personali, compreso il profilo della sicurezza.

Da segnalare la precisazione del Garante fornita in data 10 dicembre 2009, secondo cui, in vista della scadenza del 15 dicembre, termine entro il quale imprese e altri soggetti interessati dovevano adeguarsi alle prescrizioni impartite a suo tempo in materia di amministratori di sistema, è stato ritenuto opportuno precisare alcuni aspetti, anche allo scopo di evitare ingiustificati oneri per le aziende.
L'Autorità, nel rilevare il generale impegno da parte delle imprese ad adempiere alle prescrizioni impartite con il provvedimento del 27 novembre 2008, ha infatti constatato che informazioni imprecise o anche talune azioni promozionali da parte di consulenti rischiano di disorientare alcune aziende, soprattutto quelle di piccole dimensioni, esponendole a immotivati aggravi economici. L'Autorità ha inteso, dunque, ribadire quanto segue:

- le prescrizioni riguardano solo quei soggetti che, nel trattare i dati personali con strumenti informatici, devono ricorrere o abbiano fatto ricorso alla figura professionale dell'amministratore di sistema o a una figura equivalente.
- le prescrizioni non si applicano, invece, a quei soggetti anche di natura associativa che, generalmente dotati di sistemi informatici di modesta e limitata entità e comunque non particolarmente complessi, possano fare a meno di una figura professionale specificamente dedicata alla amministrazione dei sistemi o comunque abbiano ritenuto di non farvi ricorso.

Per quanto concerne, infine, gli aspetti tecnici del provvedimento (in particolare, la conservazione dei log degli accessi effettuati dagli amministratori di sistema), il Garante ha ricordato come l'adeguamento possa avvenire anche con soluzioni a basso costo, validamente proposte e disponibili in rete (per esempio basate su *software* gratuito, anche con licenze di tipo *open source*), che possono costituire valide alternative all'impiego di prodotti commerciali o di apparati più sofisticati.

Lo Studio rimane a disposizione per ogni ulteriore chiarimento.
Cordiali saluti.

firma

Società …….
Sede legale …….
Sede amministrativa ……..
Codice Fiscale ……..

Documento Programmatico sulla Sicurezza nel Trattamento dei Dati Personali

ai sensi e per gli effetti del D.Lgs. n.196 del 30 giugno 2003

Anno ...

PREMESSA **11**

1. ELENCO DEI TRATTAMENTI DI DATI PERSONALI **12**

2. DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ **14**

3. ANALISI DEI RISCHI **17**

3.1 Conservazione dei dati 17
3.2 Sicurezza logistica 17
3.3 Sicurezza informatica ed elettronica 18
3.4 Analisi dei rischi 19

4. MISURE IN ESSERE E DA ADOTTARE **22**

5. RIPRISTINO DELLA DISPONIBILITÀ DEI DATI. **24**

6. PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI. **25**

7. TRATTAMENTI AFFIDATI ALL'ESTERNO. **26**

PREMESSA

Il presente Documento, di seguito denominato per brevità DPS, viene redatto in aderenza alle disposizioni di cui al D.Lgs. n.196/03 ed è articolato nelle seguenti sezioni:

sezione	Contenuto
1	Elenco dei trattamenti di dati personali
2	Distribuzione dei compiti e delle responsabilità
3	Analisi dei rischi
4	Misure esistenti e da adottare
5	Criteri e modalità di ripristino della disponibilità dei dati
6	Pianificazione degli interventi formativi
7	Trattamenti affidati all'esterno

Solo per gli organismi sanitari e gli esercenti le professioni sanitarie è necessario prevedere anche la seguente ulteriore sezione:

8	Cifratura dei dati o separazione dei dati identificativi

Il presente Documento viene redatto da …….. nella sua qualità di …… (*titolare/responsabile*) della sicurezza della società / dello studio …….., che provvede a sottoscriverlo in calce.

Il DPS è inoltre corredato dalla seguente documentazione, che si riporta in allegato:

Selezionare, dall'elenco, i documenti che effettivamente si intende allegare, integrando con gli ulteriori documenti che si intende accludere.

- *Fac-simile* di informativa
- *Fac-simile* di lettera di incarico al Responsabile del trattamento dati
- *Fac-simile* di lettera di incarico all'Incaricato del trattamento dati
- *Fac-simile* di autorizzazione al trattamento da parte dell'interessato
- Organigramma *ex* D.Lgs. n.196/03
- Piantina della Struttura aziendale
- Certificato conformità impianti
- Elenco nominativo dei preposti alla prevenzione e sicurezza
- Caratteristiche tecniche dei *Personal Computer* di dotazione
- Dettaglio *Personal Computer*
- Informazione per la gestione della *password* del Sistema Operativo
- Documento previsto dal Provvedimento del Garante del 29/04/04 per la videosorveglianza
- D.Lgs. n.196 del 30 giugno 2003, artt.7 e 13
- DPR 14 novembre 2002 n.313, art.3
- Codice di Procedura Penale, artt.60 e 61
- ……..

1. ELENCO DEI TRATTAMENTI DI DATI PERSONALI

La società / Lo studio ……., tratta i seguenti **dati ordinari**:

Selezionare, tra le seguenti tipologie di dati, integrando opportunamente in funzione dei trattamenti effettuati presso la realtà per cui si redige il DPS

- dati personali non sensibili dei clienti, dei fornitori, dei soci, o di terzi ricavati o ricavabili da elenchi pubblici, albi professionali o camerali, visure e certificati camerali;
- dati personali non sensibili dei clienti, soci, forniti al fine di espletare gli incarichi affidati al titolare del trattamento, compresi i dati sul patrimonio o sulla situazione economica o necessari per fini fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi;
- dati personali non sensibili di fornitori, affidati al titolare del trattamento al fine della reperibilità e della corrispondenza con gli stessi, nonché per fini contabili, fiscali, o di natura bancaria, o necessari per fini fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi;
- dati personali non sensibili di soci, forniti dai clienti per l'espletamento degli incarichi affidati al titolare del trattamento, o necessari per fini fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi;
- dati personali non sensibili di soggetti terzi, forniti dai clienti per l'espletamento degli incarichi affidati al titolare del trattamento, o necessari per fini fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi;
- dati personali non sensibili dei dipendenti e dei collaboratori, necessari al regolare svolgimento del rapporto di lavoro o di collaborazione, alla reperibilità e alla corrispondenza con gli stessi, o richiesti ai fini fiscali, previdenziali, giuslavoristici, nonché quelli affidati al datore di lavoro per esigenze di natura bancaria.
- dati personali relativi ai rapporti con le banche;
- dati personali relativi alle relazioni con le assicurazioni RC e infortuni;
- dati personali relativi ai rapporti con Enti Pubblici quali Regione Emilia Romagna, Ministeri, Provincia, Comune ecc;
- dati personali relativi alla gestione delle procedure di qualità, anche in conseguenza di indicazioni fornite dall'Ente di Certificazione;
- dati personali relativi al mercato a titolo di *benchmarking*.
- ……..

La società / Lo studio …….. tratta i seguenti **dati sensibili**:

Selezionare, tra le seguenti tipologie di dati, integrando opportunamente in funzione dei trattamenti effettuati presso la realtà per cui si redige il DPS

- dati sensibili del personale dipendente, quali quelli necessari al rapporto di lavoro, o richiesti ai fini fiscali, previdenziali e giuslavoristici;
- dati sensibili dei clienti, relativi a ……...;
- dati sensibili dei soci, quali quelli necessari al rapporto di lavoro, richiesti ai fini fiscali, previdenziali e giuslavoristici;
- dati sensibili connessi alle relazioni con le assicurazioni RC e infortuni;
- dati sensibili connessi con i rapporti con Enti Pubblici quali Regione Emilia Romagna, Ministeri, Provincia, Comune ecc;
- ……

La società / Lo studio …….. tratta i seguenti **dati giudiziari**:

Selezionare, tra le seguenti tipologie di dati, integrando opportunamente in funzione dei trattamenti effettuati presso la realtà per cui si redige il DPS

- dati giudiziari del personale dipendente, OVE necessari al rapporto di lavoro, o richiesti ai fini previdenziali e giuslavoristici, quali ….;
- dati giudiziari dei clienti, quali ……;
- dati giudiziari dei fornitori, quali ……;
- dati giudiziari dei soci, quali ……;
- dati giudiziari di terzi, quali ……;
- …

Nella tabella 1.1 che segue si elencano schematicamente i trattamenti esistenti alla data di redazione e sottoscrizione del DPS, compresa ogni utile informazione idonea ad identificare inequivocabilmente il trattamento, la struttura aziendale all'interno della quale il trattamento viene eseguito, gli strumenti utilizzati nel trattamento. Per questi ultimi, ove necessario, sono indicati ulteriori elementi necessari alla miglior individuazione di quanto tecnicamente utilizzato a supporto del singolo trattamento.

Tabella 1.1 - Elenco dei trattamenti					
1	Identificativo		Descrizione		
Natura dei dati (1)	[_] Personali [_] Sensibili		[_] Giudiziari	Data di aggiornamento	
Strutture aziendali (2)			Strutture esterne (3)		
Strumenti utilizzati:					
Banca dati utilizzata		Ubicazione fisica supporti	Tipo dispositivi di accesso	Tipo di interconnessione	
2	Identificativo		Descrizione		
Natura dei dati (1)	[_] Personali [_] Sensibili		[_] Giudiziari	Data di aggiornamento	
Strutture aziendali (2)			Strutture esterne (3)		
Strumenti utilizzati:					
Banca dati utilizzata		Ubicazione fisica supporti	Tipo dispositivi di accesso	Tipo di interconnessione	

Note:
(1) barrare la casella interessata
(2) va riportata l'indicazione di massima del reparto/ufficio/funzione aziendale coinvolta; questa casella è correlata all'indicazione analitica dei soggetti interessati evidenziata nella sezione che segue (2, tabella 2.1)
(3) riportare gli eventuali soggetti esterni alla società che operativamente effettuato il trattamento o parte di esso

Di seguito si propone un esempio di compilazione della tabella:

Tabella 1.1 - Elenco dei trattamenti					
1	Identificativo	**DIP/01**	Descrizione	Dati del personale dipendente	
Natura dei dati (1)	**[X]** Personali **[X]** Sensibili		[_] Giudiziari	Data di aggiornamento	28/03/10
Strutture aziendali (2)	Divisione amministrativa		Strutture esterne (3)	Consulente del Lavoro Dott. Rossi Paolo	
Strumenti utilizzati:					
Banca dati utilizzata		Ubicazione fisica supporti	Tipo dispositivi di accesso	Tipo di interconnessione	
		1) Armadio chiuso a chiave nell'ufficio del personale 2) Cassaforte in segreteria (dati per L. n.626)			
Foglio di lavoro \server\dipendenti.xls		Memorizzazione sul server, Stanza EDP, chiusa a chiave, non accessibile	Riservato alla divisione amministrativa; accesso mediante *password*.	Connessione in rete TCP/IP	

2. DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ

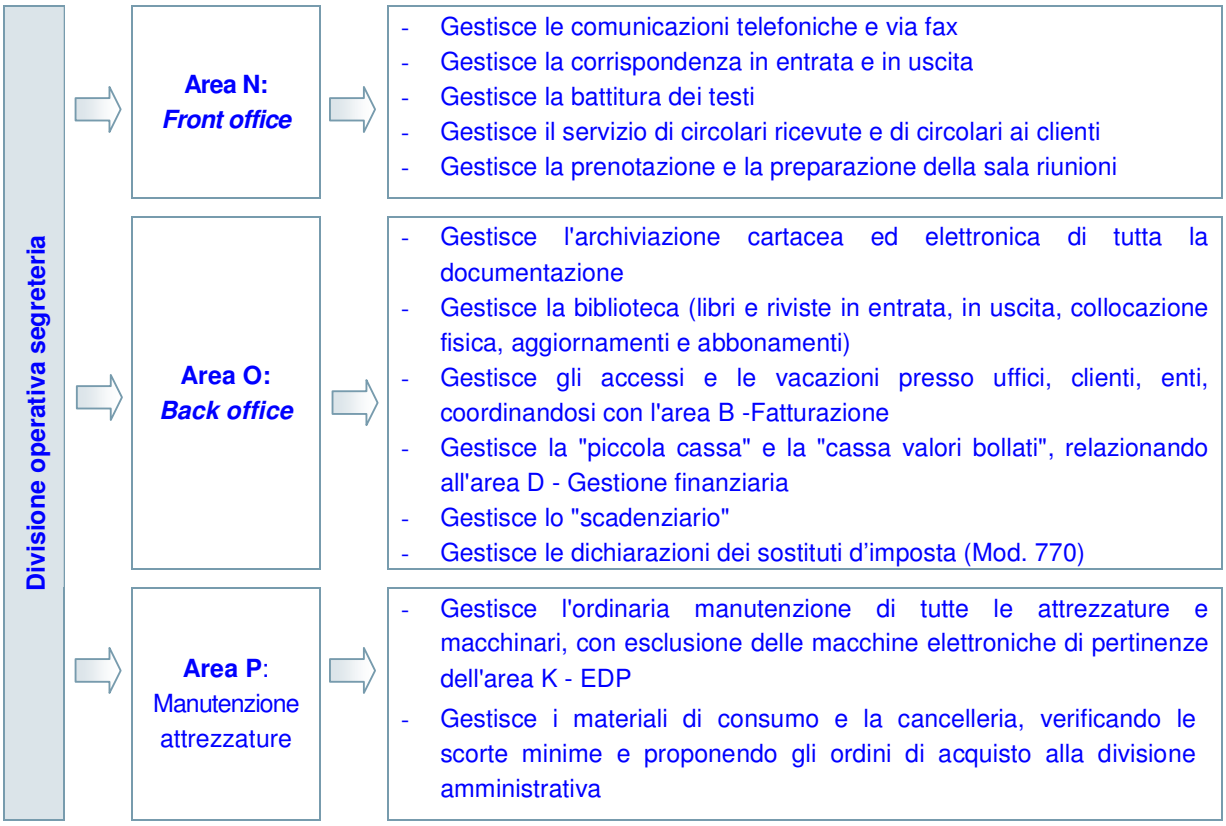
La società / Lo studio …… è già dotata / dotato di un organigramma e di un mansionario che di seguito viene integralmente riportato. Anche in questo Documento i riferimenti ai componenti strutturali vanno fatti a questo documento:

Qui occorre inserire un organigramma e mansionario aziendale.
Di seguito si propone un esempio di mansionario, del tutto indicativo, che è da completare e modificare in funzione delle specifiche caratteristiche aziendali

Divisione Amministrativa

Area A: Contabilità e bilancio	- Sovrintende alla redazione della contabilità, concordando con la persona addetta metodologie e scritturazioni - Predispone la bozza di bilancio da sottoporre al Consiglio di Amministrazione - Sovrintende alla redazione del bilancio definitivo da sottoporre all'approvazione dei soci - Sovrintende alla redazione delle dichiarazioni fiscali
Area B: Fatturazione e valorizzazione prestazioni	- Sovrintende alla redazione delle fatture - Coordina l'attività di reperimento dei dati al fine della corretta fatturazione - Coordina l'attività di controllo interno delle prestazioni fatturate - Pianifica e coordina i *budget* annuali degli importi da fatturare - Sovrintende al controllo del fatturato rispetto agli impegni contrattuali assunti (mandati) - Sovrintende alla gestione delle anticipazioni di cassa - Coordina e trasmette i *report* periodici - Coordina l'attività di recupero crediti
Area C: Pianificazione e controllo di gestione	- Predispone il budget preventivo dei costi - Sovrintende al controllo di gestione - Autorizza gli ordini di acquisto, provenienti dalle diverse aree
Area D: Gestione finanziaria	- Sovrintende alla gestione della cassa - Sovrintende alla gestione delle anticipazioni - Sovrintende alle operazioni eseguite tramite banca - Cura il rapporto con gli istituti di credito - Coordina e trasmette i *report* finanziari periodici
Area E: Personale	- Sovrintende alla monitorizzazione delle presenze mensili - Cura i rapporti con il consulente del lavoro - Coordina le ferie, i permessi, le assenze del personale - Sovrintende alla gestione delle assenze - Sovrintende alla consegna dei cedolini mensili, e di altri eventuali documenti


Divisione Direzionale
Area F: Formazione e Risorse Umane
- Coordina l'attività di selezione del personale
- Sovrintende alla formazione, sia interna che esterna, delle risorse umane, sia in fase di *start-up* che periodicamente, coordinando l'utilizzo di persone e strumenti formativi
- Coordina l'attività di valutazione periodica del personale
- Sovrintende alla gestione del registro degli infortuni professionali
Area G: Marketing
- Pianifica e sovrintende all'attività di promozione dell'immagine
- Coordina l'attività di "*customer satisfaction*"
Area H: Sicurezza
- Sovrintende alla corretta gestione degli adempimenti legati alla Legge n.626 (sicurezza sul lavoro)
- Sovrintende alla corretta gestione degli adempimenti legati al D.Lgs. n.196/03 (*Privacy*)
Area I: Gestione del Patrimonio
- Sovrintende alla manutenzione dei beni
- Pianifica la sostituzione degli stessi beni
- Sovrintende alla disposizione degli ambienti di lavoro
- Sovrintende alla preservazione dei beni contro furto, incendio, intrusione
- Sovrintende alla gestione degli impianti di allarme
Area J: TQM
- Coordina l'acquisizione, la produzione, la divulgazione, il corretto utilizzo delle procedure
- Sovrintende alla predisposizione dei documenti da utilizzare, previa approvazione della Direzione Generale
Area K: EDP
- Gestisce la manutenzione, l'upgrade, la sostituzione, del materiale elettronico
- Gestisce tutto il *software* dello studio, compresa la gestione delle licenze d'uso dei programmi
- Coordina e sovrintende al *backup* degli archivi elettronici
- Coordina la realizzazione, interna o esterna, di strumenti e procedure informatiche, su sollecitazione propria o delle diverse divisioni ed aree
Divisione operativa Segmento 1
Area L
- …
Divisione operativa Segmento 2
Area M
- …



Considerando, quindi, le risorse a disposizione della struttura aziendale, nella tabella 2.1 sono specificatamente riportate le informazioni in materia di sicurezza del trattamento dei dati.

Tabella 2.1 – Strutture preposte ai trattamenti				
1	Struttura (1)		Data di aggiornamento	
Dati riferiti ai singoli trattamenti				
Responsabile		Trattamento operato (2)	Compiti della struttura	

Note:
indicare la struttura aziendale, coordinando il dato con quanto già redatto nella precedente sezione in tabella 1.1
indicare il trattamento, così come identificato in tabella 1.1

Di seguito si propone un esempio di compilazione della tabella

1	Struttura (1)	Divisione amministrativa area E	Data di aggiornamento	28/03/10
Dati riferiti ai singoli trattamenti				
Responsabile		Trattamento operato (2)	Compiti della struttura	
Mario Rossi		**DIP/01**	Intera gestione del personale come risulta dal mansionario	

3. ANALISI DEI RISCHI

Conservazione dei dati

I **dati personali** trattati sono tutti archiviati al termine della pratica e conservati:

Selezionare, tra le seguenti tipologie di dati, integrando opportunamente in funzione delle specifiche caratteristiche della realtà per cui si redige il DPS

- in fascicoli riposti in armadi dotati di chiusura, in locali protetti;
- in fascicoli riposti in armadi dotati di chiusura;
- in fascicoli riposti in armadi non dotati di chiusura;
- tramite *personal computer* connessi in rete;
- tramite *personal computer* non connessi in rete.

I **dati sensibili** trattati sono tutti archiviati al termine della pratica e conservati:

Selezionare, tra le seguenti tipologie di dati, integrando opportunamente in funzione delle specifiche caratteristiche della realtà per cui si redige il DPS

- in fascicoli riposti in armadi dotati di chiusura, in locali protetti, archiviati al termine della pratica;
- in fascicoli riposti in armadi dotati di chiusura;
- tramite *personal computer* connessi in rete;
- tramite *personal computer* non connessi in rete

I **dati giudiziari** trattati sono conservati:

Selezionare, tra le seguenti tipologie di dati, integrando opportunamente in funzione delle specifiche caratteristiche della realtà per cui si redige il DPS

- in fascicoli riposti in armadi dotati di chiusura, in locali protetti, archiviati al termine della pratica;
- in fascicoli riposti in armadi dotati di chiusura;
- tramite *personal computer* connessi in rete;
- tramite *personal computer* non connessi in rete

Sicurezza logistica

La sede della società / dello studio, ove vengono trattati i dati, è ubicata ……..

Per esempio in un condominio in zona periferica/industriale/…, o in un singolo stabile sito in ……),

è dotata di:

Selezionare, tra le seguenti tipologie, integrando opportunamente in funzione delle specifiche caratteristiche della realtà per cui si redige il DPS

- portone blindato;
- porta scorrevole a vetri;
- porta con chiusura automatica;
- videocitofono;
- sorveglianza notturna;
- di sistema di allarme;
- ……

Di seguito si propone una breve descrizione della piantina aziendale….

Proporre una breve descrizione dei locali di cui è composto lo stabile, specificando, ufficio per ufficio se vi vengono trattati dati personali, sensibili o giudiziari.

I locali aziendali sono dotati di serratura con chiave. Così quindi anche per:

Selezionare, tra i seguenti locali, integrando opportunamente in funzione delle specifiche caratteristiche della realtà per cui si redige il DPS

- l'archivio;
- il centro elaborazione dati;
- il locale che accoglie il *server*;
- il locale che accoglie le copie dei dati informatici;
- …..

L'archivio è dotato di cassaforte con chiusura a chiave (*o a combinazione, ecc…*).

Sicurezza informatica ed elettronica

Ogni postazione è dotata di *personal computer* in rete e connesso ad Internet.

Alternativamente, indicare quali postazioni sono dotate di personal computer in rete e quali sono connessi ad internet.

La società / Lo studio è inoltre dotato dei seguenti dispositivi:

Selezionare, tra i seguenti dispositivi, integrando opportunamente in funzione delle specifiche dotazioni della realtà per cui si redige il DPS

- n…..stampanti;
- n….. fax;
- n…. scanner;
- n…. fotocopiatrici;
- n…..trita documenti
- …..

Le dotazioni informatiche sono collocate negli uffici, mentre nell'area produzione vi sono stazioni di controllo dotate solo di alcuni programmi tecnici; ne consegue che l'utilizzo dei *personal computer* è possibile da parte del personale dipendente o da esterni autorizzati e quindi non da parte del pubblico.

Verificare se pertinente alla realtà per cui si sta redigendo il DPS e modificare/integrare opportunamente

Di seguito si dettagliano i *software* utilizzati in azienda/studio, specificando quali dati personali vengono trattati da ciascuno di essi.

SOFTWARE …..

Inserire il nome del *software*

È il programma che consente di ……

Fornire una breve descrizione delle funzionalità del programma

Attraverso tale software vengono trattati i seguenti dati personali: ……

Fornire una breve elencazione dei dati personali trattati attraverso tale programma

SOFTWARE …..

Inserire il nome del software

È il programma che consente di ……

Fornire una breve descrizione delle funzionalità del programma

Attraverso tale *software* vengono trattati i seguenti dati personali: ……

Fornire una breve elencazione dei dati personali trattati attraverso tale programma

Tre sono i possibili livelli di *password* attualmente attivati:

- ***Password* di BIOS (*Basic Input/Output System*)**
  È stata attivata nei seguenti *personal computer*:
  - …..
  - …..

Fornire un elenco riassuntivo dei *personal computer* dotati di *password* di Bios

Essa viene modificata nei tempi ritenuti opportuni da parte dell'utilizzatore e comunque almeno ogni tre mesi.

Verificare che sia stata disposizione a che venga modificata almeno ogni tre mesi

- ***Password* del Dominio**
  Ogni dipendente può accedere a qualsiasi *personal computer* solo e soltanto segnalando la propria *user id* e *password*, che gli consentono da qualsiasi postazione di accedere soltanto alle informazioni cui egli è stato abilitato.
  Si tratta di una *password* che non è conosciuta, né è conoscibile da alcuno, salvo gli interessati.
  Il processo di cambiamento della *password* viene gestito in via automatica, con conseguente obbligo da parte degli utenti di modificarla ogni tre mesi. È stato a ciò predisposto un sistema di avvertimento che perviene sul *personal computer* di ogni singolo utente in prossimità della scadenza e che obbliga all'immissione di una *password* diversa da quella precedentemente immessa e dotata delle specifiche previste dal D.Lgs. n.196/03.

Verificare il rispetto di quanto qui scritto ed eventualmente modificare in funzione delle specificità aziendali

- ***Password* di programma**
  Per ciascun programma, la gestione della scadenza delle *password* è lasciata all'autonomia di ciascun utente che è stato debitamente edotto dell'impossibilità di avvalersi del medesimo codice per oltre tre mesi.

Verificare il rispetto di quanto qui scritto ed eventualmente modificare in funzione delle specificità aziendali

In caso di assenza o impedimento prolungato dell'Incaricato depositario delle *password* di accesso ai vari sistemi, il Responsabile Sistemi Informativi, o suo Incaricato, può accedere alle informazioni, avvalendosi delle proprie password di amministratore.

Verificare il rispetto di quanto qui scritto ed eventualmente modificare in funzione delle specificità aziendali

Analisi dei rischi

È stata compiuta l'analisi dei rischi, avendo attenzione alla tipologia degli eventi che possono generare danni e che comportano quindi rischi per la sicurezza dei dati personali, nonché all'impatto sulla sicurezza dei dati, in relazione a ciascun evento e alla gravità e probabilità stimata dell'evento stesso. Per ciascun evento probabile, si è considerata la contromisura adottata o da adottare.
Sinteticamente, si valuta **basso** il rischio legato alla gestione dei seguenti trattamenti (identificati come da tabella 1.1, alla quale si rimanda per i dati caratteristici):

trattamenti con rischio basso	
Identificativo	Descrizione di massima

Per esempio:

DIP/01	Dati comuni dei dipendenti

Sinteticamente, si valuta **medio** il rischio legato alla gestione dei seguenti trattamenti (identificati come da tabella 1.1, alla quale si rimanda per i dati caratteristici):

trattamenti con rischio medio	
Identificativo	Descrizione di massima

Sinteticamente, si valuta **alto** il rischio legato alla gestione dei seguenti trattamenti (identificati come da tabella 1.1, alla quale si rimanda per i dati caratteristici):

trattamenti con rischio alto	
Identificativo	Descrizione di massima

Per esempio:

Identificativo	Descrizione di massima
DIP/01	Dati sensibili dei dipendenti (fascicoli inviati dal medico del lavoro e conservati in busta sigillata)

Di seguito sono elencati gli eventi che possono verificarsi, suddivisi in base alla natura della causa scatenante (operatori, strumenti elettronici, struttura aziendale); per ciascuno è specificato l'identificativo della contromisura, per il cui dettaglio si rimanda alla successiva sezione 4.

La tabella che segue è quella predisposta dall'ufficio del Garante della *Privacy* nella bozza di DPS del 13 maggio 2004; come indicato dal medesimo ufficio, si tratta solo di una lista esemplificativa e non esaustiva, da prendere come base di partenza per ogni utile implementazione legata alle specifiche esigenze e peculiarità di ciascun soggetto interessato alla redazione del DPS

Tabella 3.1 - Analisi dei rischi			
Evento		**Descrizione**	**Contromisura**
Comportamenti degli operatori	Furto di credenziali di autenticazione		
	Carenza di consapevolezza, disattenzione o incuria		
	Comportamenti sleali o fraudolenti		
	Errori materiali		
Eventi relativi agli strumenti	Azione di *virus* informatici		
	Spamming o altre tecniche informatiche di sabotaggio		

	Malfunzionamento degli strumenti elettronici		
	Accessi esterni non autorizzati		
	Intercettazione di informazioni in rete		
Eventi relativi al contesto strutturale	Accessi non autorizzati a locali ad accesso ristretto		
	Asportazione e furto di strumenti contenenti dati		
	Eventi distruttivi, naturali o accidentali o dolosi, o per incuria		
	Guasto ai sistemi complementari (impianti elettrico, condizionamento)		
	Errori umani nella gestione della sicurezza fisica		

4. MISURE IN ESSERE E DA ADOTTARE

A fronte dell'analisi dei rischi di cui alla precedente sezione 3, di seguito si descrivono le misure di sicurezza adottate dalla società / dallo studio.

Di seguito si propone un esempio, che deve essere opportunamente adattato alla realtà per cui si redige il DPS

Misura 1. *Antivirus*
Ogni singolo computer è dotato di dispositivo *antivirus*, che viene aggiornato con funzione automatica e con scansione per ogni aggiornamento antivirus, e in ogni caso almeno settimanalmente, in orario compatibile con il fatto che il computer non sia spento (in questo caso la scansione avverrà alla successiva accensione).

Misura 2. *Firewall*
Sul server è stato installato *firewall* con le seguenti caratteristiche: …

Misura 3. *Backup*
È stato disposto l'obbligo di provvedere ad un *backup* settimanale dei dati e dei sistemi installati sul *server* su:
- cd rom
- cassette,
- ……

Selezionare l'opzione presente nelle realtà per cui si redige il DPS

i quali vengono conservati e chiusi:
- in un armadio chiuso a chiave e protetto da agenti ignifughi,
- in cassaforte chiusa a chiave e protetta da agenti ignifughi,
- in cassaforte esterna chiusa a chiave e protetta da agenti ignifughi,
- ….

Selezionare l'opzione presente nelle realtà per cui si redige il DPS

e si è data disposizione di verificare, effettuato il *backup*, la leggibilità del supporto e che una volta a settimana si proceda a verifica a campione della leggibilità dei dati.

Misura 4. *Screensaver*
Tutti gli utilizzatori di strumenti elettronici non devono lasciare incustodito, o accessibile, lo strumento stesso. A tale riguardo, per evitare errori e dimenticanze, è stato predisposto lo *screensaver* automatico dopo … minuti di non utilizzo, con ulteriore *password* segreta per la prosecuzione del lavoro.

Misura 5. Autenticazione informatica
Tale misura è stata adottata dotando ciascun incaricato di una *password* di almeno 8 caratteri. Detta *password* non contiene, né conterrà, elementi facilmente ricollegabili all'organizzazione o alla persona del suo utilizzatore, né alla società/allo studio. La stessa viene autonomamente scelta dall'incaricato e dallo stesso custodita in una busta chiusa che viene consegnata al titolare/responsabile del trattamento, il quale provvede a metterla nella cassaforte/luogo sicuro in un plico sigillato. Ogni tre mesi ciascun incaricato provvede a sostituire la propria *password*. Si è altresì disposto che le *password* vengano automaticamente disattivate dopo tre mesi di non utilizzo.

Misura 6. Archiviazione
Si è disposto che non siano lasciati 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.

Misura 7. Stampe centralizzate
Quando è dato un ordine di stampa, il documento stampato dovrà essere prontamente prelevato dall'interessato o consegnato allo stesso.

Misura 8. *Fax*
I fax arrivano in zona protetta, accessibile solo dagli incaricati dell'area della segreteria, con la parte scritta verso il basso per evitare di rimanere in vista incidentalmente.

Misura 9. Archivio
Il locale destinato all'archivio è sempre chiuso a chiave. L'incaricato preposto dovrà controllare l'accesso all'archivio. Fuori dall'orario di lavoro l'accesso all'archivio è consentito esclusivamente previa registrazione.

Misura 10. Distruzione documenti
Si è data istruzione che il materiale cartaceo asportato e destinato allo smaltimento dei rifiuti sia riposto negli appositi sacchi di plastica, previo passaggio nelle apposite macchine tagliadocumenti (in dotazione almeno in misura di uno per ciascun ufficio) 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.

Misura 11. Eventi naturali
La società ha provveduto ad adottare le disposizioni di sicurezza stabilite dalla L. n.626/94 e successive modifiche e integrazioni.

5. RIPRISTINO DELLA DISPONIBILITÀ DEI DATI

Oltre alla procedura di *backup* (vedasi Misura 3 della precedente sezione) la società / lo studio ha approntato la seguente procedura di "*disaster recovery*", vale a dire di ripristino della disponibilità dei dati.

Di seguito si propone l'ipotesi in cui avvalendosi di consulenti informatici esterni all'azienda essi risultano coinvolti nelle procedure di sicurezza. Tale sezione dovrà quindi essere opportunamente adattata alla specifica realtà dell'azienda per cui si redige il DPS

Si premette che ci si avvale anche della consulenza informatica della società ……., come risulta anche dalla lettera di assunzione di incarico sottoscritta in data ……
Nell'ipotesi di distruzione o danneggiamento dei dati o degli strumenti elettronici:

- deve essere avvertito il titolare del trattamento dei dati e l'incaricato che ha in custodia il CD ROM / cassette di *back up* nonché i CD ROM contenenti i vari *software* installati sugli strumenti elettronici;
- ci si deve rivolgere immediatamente al tecnico manutentore del consulente informatico sollecitandone al più presto l'assistenza;
- ciascun incaricato deve provvedere ad inventariare nella maniera più precisa possibile il lavoro svolto dal momento dell'ultimo *back up* al momento della rottura irreversibile;
- si devono reinstallare i programmi danneggiati o distrutti, sempre che non sia necessario sostituire l'intero *hardware*, provvedere a reinstallare tutti i dati contenuti nel CD ROM / nelle cassette di *back up*;
- si deve provvedere all'aggiornamento dei sistemi operativi una volta reinstallati;
- al fine di evitare eventi di perdita e di danneggiamento degli strumenti elettronici e dei dati in essi contenuti, si prevede che per due volte all'anno sia effettuata manutenzione in modo adeguato dal tecnico incaricato.

6. PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI

Nell'ambito delle procedure di tutela della sicurezza dei dati trattati dalla società / dallo studio si è proceduto a stilare il piano dell'impegno formativo che si prevede di sostenere in attuazione della normativa sulla *Privacy*, secondo la tabella che segue.

Tabella 6.1 – Interventi formativi previsti

Corso di formazione	Descrizione sintetica	Categorie interessate	Numero soggetti interessati	Calendario date

7. TRATTAMENTI AFFIDATI ALL'ESTERNO

In quest'ultima sezione vengono fornite, con l'ausilio della successiva tabella 7.1, tutte le indicazioni necessarie ad identificare i dati trattati all'esterno, nonché i soggetti coinvolti.
Si premette che è stata predisposta idonea documentazione rilasciata dai soggetti cui le varie attività sono affidate dalla quale risulta:

- che il terzo dichiara di essere consapevole che i dati da lui trattati nell'espletamento dell'incarico ricevuto sono dati personali e, come tali, sono soggetti alla disciplina di cui al D.Lgs. n.196/03 (Codice per la protezione dei dati personali);
- che il terzo dichiara di ottemperare agli obblighi previsti dal predetto D.Lgs. n.196/03;
- che il terzo dichiara di adottare ogni istruzione ricevuta dal titolare del trattamento;
- che il terzo si impegna a relazionare al titolare in ordine alle misure di sicurezza da lui adottate, dando notizia al committente circa le situazioni di pericolo per i dati in cui potrebbe imbattersi;
- che il terzo dichiara di riconoscere il diritto del committente alla verifica periodica dell'applicazione delle norme di sicurezza adottate.

Verificare che quanto sopra sia stato effettivamente effettuato

Tabella 7.1 – Trattamenti affidati all'esterno

Attività esternalizzata	Descrizione sintetica	Dati sensibili e giudiziari interessati	Soggetto esterno incaricato	Descrizione criteri per l'adozione delle misure di sicurezza	Date delle verifiche

Luogo e data

_____

Firma

_____

Oggetto: SCADENZARIO DEI PRINCIPALI ADEMPIMENTI *PRIVACY*

Scadenza	Formalità da effettuare	Formulario allegato
Giornalmente	Salvataggio dei dati informatici	
Settimanalmente	Verifica della correttezza dei salvataggi effettuati su supporto informatico	
Trimestralmente	Modifica delle *password*	
Periodicamente	Verifica della presenza delle apposite diciture su tutti i documenti aziendali/di Studio (fax, mail, *fac simili*, fatture, ddt, ecc.)	
Periodicamente	Verifica degli strumenti elettrici ed elettronici presenti in Azienda/Studio	
Periodicamente	Controllo dell'operato degli Incaricati / dei Responsabili per il rispetto delle del D.Lgs. n.196/03	
Annualmente	Effettuazione di un percorso di formazione destinato agli Incaricati/ai Responsabili	
31 marzo di ogni anno	Redazione e Aggiornamento del Documento Programmatico per la sicurezza dei dati (DPS)	Sì
Data di redazione del bilancio	Informativa contenuta nel Bilancio, in merito all'avvenuto adempimento delle disposizioni previste dal D.Lgs. n.196/03	
Prima di un colloquio con un potenziale Dipendente	Compilazione a cura del potenziale Dipendente dell'*Informativa per Domanda di Lavoro*	Sì
All'atto dell'assunzione di un Dipendente/ dell'avvio di una nuova collaborazione	Consegna della *Lettera di nomina al ruolo di Incaricato / Responsabile*	Sì
	Consegna delle *Istruzioni per la custodia della password*	Sì
In caso di modifica dell'Organigramma aziendale	Consegna della *Lettera di nomina al ruolo di Incaricato/Responsabile,* ove non nominato precedentemente	Sì
	Consegna delle *Istruzioni per la custodia della password,* ove non consegnate precedentemente	Sì
All'atto della collaborazione con nuovi Clienti / Fornitori	Consegna del modulo *Informativa a Clienti e Fornitori* e ottenimento della stessa, controfirmata	Sì
All'atto dell'installazione di sistemi di videosorveglianza	Redazione di apposito Documento sulle modalità di effettuazione dell'attività di videosorveglianza	
All'atto della costruzione di siti internet aziendali / di Studio	Predisposizione di apposita *Privacy Policy* da inserire nel sito	
Al verificarsi dell'evento	Eventuali comunicazioni al Garante per l'ottenimento di autorizzazioni specifiche *(per esempio uso di impronte digitali, ecc.)*	

Oggetto: *FAC-SIMILE* DI INFORMATIVA DATI PERSONALI PER DIPENDENTI E COLLABORATORI

NOTE METODOLOGICHE

Nel documento di seguito proposto:

- le parti in **nero** sono quelle generalmente idonee per la totalità delle imprese interessate;
- le parti in **blu** sono le sezioni che possono essere differenti, realtà per realtà;
- le parti in ***bordeaux*** e quelle su sfondo grigio sono le note operative, utili per la compilazione, ma da cancellare in sede di definizione del presente documento.

D.Lgs. n.196/03 - Codice in materia di protezione dei dati personali

Ai sensi dell'art.13 del D.Lgs. n.196/03, La informiamo che i dati personali da Lei trascritti nel presente modulo e i dettagli aggiunti dalla Persona con la quale conferisce saranno oggetto di trattamento anche con l'ausilio di strumenti informatici, in relazione alle sole finalità di ricerca e selezione del Personale, con l'utilizzo di mezzi conformi a quanto previsto dal D.Lgs. n.196/03.

Il conferimento dei dati è facoltativo; resta inteso che l'eventuale mancato conferimento del consenso al trattamento, comporterà l'impossibilità di condurre la selezione nei Suoi confronti. Detti dati potranno essere trattati dalla nostra Azienda / dal nostro Studio e da altri soggetti esterni per le medesime finalità sopra riportate.

La preghiamo di evitare di riportare dati idonei a rilevare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni ed organizzazioni a carattere religioso, filosofico, politico o sindacale, i dati personali idonei a rivelare la vita sessuale nonché lo stato di salute, a meno che questi non costituiscano titolo per ricoprire la posizione ricercata, fermo restando che il Suo stato di salute deve essere compatibile con la posizione cui Lei aspira.

Titolare e Responsabile del trattamento

Ai sensi del D.Lgs. n.196/03:

- Titolare del Trattamento è _____, nella persona del suo Legale Rappresentante;

Segnalare il nome del Titolare del trattamento dei dati (in genere è la Società / lo Studio stesso) ed il recapito cui potersi rivolgere.
Qualora il Titolare non sia la Società / lo Studio, cancellare la sezione successiva "nella persona del suo Legale Rappresentante"

- Responsabile del Trattamento dei Suoi dati è _____.

Segnalare il nome del Responsabile del trattamento dei dati

Diritto di accesso ai dati personali ed altri diritti

Il D.Lgs. n.196/03, all'art.7 Le riconosce il diritto di ottenere da questa Azienda / da questo Studio la conferma dell'esistenza o meno dei dati personali che La riguardano, la relativa comunicazione, origine, finalità, modalità di trattamento, cancellazione, rettifica, aggiornamento, integrazione, nonché di opporsi in tutto o in parte al trattamento dei dati in oggetto.

Dichiarazione di consenso al trattamento dei dati personali

Preso atto di quanto sopra, consapevole dei diritti a me riconosciuti dal D.Lgs. n.196/03, in specie dall'art.7, autorizzo Codesta Azienda / Codesto Studio ed eventuali Soggetti da essa appositamente designati, al trattamento dei **dati personali** da me forniti sia con la compilazione del presente modulo che nel corso del colloquio, per le sole finalità di ricerca e selezione del Personale.

Data _____ Firma _____

Qui va apposta la firma da parte del Candidato alla selezione

Dichiarazione di consenso al trattamento dei *dati sensibili e/o giudiziari*

Preso atto di quanto sopra, consapevole dei diritti a me riconosciuti dal D.Lgs. n.196/03, in specie dall'art.7, autorizzo Codesta Azienda / Codesto Studio ed eventuali Soggetti da essa appositamente designati, al trattamento dei **dati sensibili e/o giudiziari** da me forniti sia con la compilazione del presente modulo che nel corso del colloquio, per le sole finalità di ricerca e selezione del Personale.

Data _____ Firma _____

Qui va apposta la firma da parte del Candidato alla selezione

Oggetto: *FAC-SIMILE* DI LETTERA DI NOMINA INCARICATI

NOTE METODOLOGICHE
Nel documento di seguito proposto:

- le parti in **nero** sono quelle generalmente idonee per la totalità delle Imprese / degli Studi, in fase di nomina dell'Incaricato;
- le parti in **blu** sono le sezioni che possono essere differenti, realtà per realtà;
- le parti in ***bordeaux*** e quelle su sfondo grigio sono le note operative, utili per la compilazione, ma da cancellare in sede di definizione della nomina dell'Incaricato

Carta intestata dell'Azienda / Studio
(soggetto per il quale si sta curando la messa a regime sulla *Privacy*)

Luogo e data, _____

Inserire Luogo e data in cui si consegna il presente incarico

Preg.mo/a Sig / Sig.ra
_____
_____

Inserire i dati anagrafici del Dipendente/Collaboratore cui qui si intende conferire l'incarico di Incaricato

OGGETTO: Nomina dell'Incaricato al Trattamento dei dati

Il / La sottoscritto / a _____
nato / a a _____il _____
Codice Fiscale _____

Qui sopra, occorre riportare i dati anagrafici del Responsabile del Trattamento dei dati aziendale/di Studio, che conferisce l'incarico di"Incaricato al trattamento dei dati". Qualora non nominato il Responsabile al Trattamento dati, si indicheranno i dati del Titolare del trattamento dati.

in qualità di Responsabile Trattamento dati _____

Qui va specificato il ruolo specifico del Responsabile che conferisce l'incarico. Per esempio: Responsabile amministrativo, Responsabile Risorse Umane, Responsabile Produzione, Responsabile Commerciale, ecc.

vista la normativa in materia di *Privacy* disciplinata dal D.Lgs. n.196/03 Codice in materia di protezione dei dati personali, con la presente nomino:

il Sig. / la Sig.ra _____
nato / a a _____il _____
Codice Fiscale _____

Qui sopra, occorre riportare i dati anagrafici del Soggetto cui si sta conferendo l'incarico di"Incaricato al trattamento dei dati".

Incaricato del Trattamento dei dati nell'ambito delle funzioni che è chiamata a svolgere in relazione al rapporto di lavoro / collaborazione / tirocinio / stage / prestazione occasionale , con le finalità e secondo le modalità stabilite, anche in futuro, dal Responsabile _____e, comunque, in modo lecito e secondo correttezza.

Selezionare tra lavoro / collaborazione / tirocinio / *stage* / prestazione occasionale, in base al rapporto esistente con il soggetto che si sta nominando.
Poi va riportato il ruolo specifico del Responsabile che conferisce l'incarico, già sopra citato. Per esempio: Responsabile amministrativo, Responsabile Risorse Umane, Responsabile Produzione, Responsabile Commerciale, ecc.

Nello svolgimento dell'attività:

- il trattamento dei dati deve essere effettuato nel rispetto di quanto previsto dal D.Lgs. n.196/03 e successive modificazioni;
- i dati personali devono essere raccolti e registrati unicamente per finalità inerenti l'attività svolta;
- Le è consentito l'accesso solo a quei dati la cui conoscenza è strettamente necessaria allo svolgimento dei compiti che Le vengono assegnati;
- Le è vietato effettuare copie, fotostatiche o di qualsiasi altra natura, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante dati personali per fini estranei alla Sua attività lavorativa e consegnare a persone non autorizzate, sottrarre, cancellare o distruggere stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento;
- è necessaria la verifica costante dei dati ed il loro aggiornamento;
- è necessaria la verifica costante della completezza e pertinenza dei dati trattati;
- occorre adottare tutte le misure di sicurezza atte ad evitare la distruzione o la perdita, anche accidentale dei dati;
- devono essere rispettate tutte le misure di sicurezza:
  - indicate nel Documento Programmatico sulla Sicurezza nel Trattamento dei Dati Personali;
  - previsti nel Regolamento *Privacy* adottato dall'Azienda / dallo Studio;
  - impartite direttamente dal Responsabile e dal Titolare;

Poiché non tutte le Aziende sono dotate di DPS e di Regolamento *Privacy*, qualora essi non fossero stati predisposti, eliminare i relativi richiami qui sopra esposti in blu

- occorre segnalare al Responsabile o, in sua mancanza, al Titolare, eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita anche accidentale dei dati, di accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta;
- al fine di evitare accessi incidentali ai dati, qualora terzi estranei (p.e. clienti, dipendenti di società esterne, ecc.) debbano accedere nell'Ufficio, occorre assicurarsi che i dati personali maneggiati e/o archiviati non siano suscettibili di indiscrete visioni raccogliendo, registrando e conservando i dati presenti negli atti e documenti contenuti nei fascicoli appositamente predisposti e nei supporti informatici, avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
- al termine della giornata lavorativa o in caso di allontanamento, le pratiche, i documenti ed eventualmente i *floppy-disk* / cd-rom / dvd di salvataggio contenenti dati personali vanno riposti in armadi, cassetti ed altri contenitori chiusi a chiave;

- i documenti che contengono dati personali o comunque di natura riservata devono essere cestinati assicurandosi preventivamente che non siano più leggibili, eventualmente ricorrendo ad apposite attrezzature (p.e. trita documenti);

Qualora non presente il trita documenti, nell'Azienda / Studio in cui opera l'Incaricato cui si sta conferendo il presente incarico, cancellare il relativo riferimento

- la trasmissione della corrispondenza ed i documenti inerenti i dati personali, quando non effettuata personalmente o tramite persone incaricate del trattamento, deve avvenire in busta chiusa e sigillata;
- Le è consentito di effettuare la comunicazione dei dati esclusivamente ai soggetti indicati dal Responsabile o dal Titolare e secondo le finalità dallo stesso stabilite;
- Le è consentito di effettuare la diffusione dei dati, secondo le finalità dallo stesso stabilite;
- occorre mantenere, la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento dell'incarico, per tutta la durata del medesimo ed anche successivamente al termine di esso;
- occorre fornire al Responsabile e al Titolare, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire di svolgere efficacemente la propria attività di controllo;
- occorre in generale, prestare la più ampia e completa collaborazione al Responsabile / Titolare al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente;

Qualora non fosse presente il Responsabile, lasciare Titolare, altrimenti depennare Titolare

- occorre consegnare ai soggetti che conferiscano per la prima volta dati personali, gli appositi moduli di raccolta del consenso predisposti dalla nostra Società / dal nostro Studio unitamente all'informativa di cui all'art.13 del D.Lgs. n.196/03, salvo che l'informativa medesima sia stata fornita direttamente dal Responsabile.

Selezionare tra Società / Studio, a seconda della realtà in cui opera l'Incaricato che si sta nominando

La presente nomina può essere revocata in ogni momento, con effetto immediato e senza obbligo di preavviso e si intende revocata automaticamente in caso di interruzione del rapporto di lavoro / collaborazione / tirocinio / *stage* / prestazione occasionale, per dimissioni / licenziamento / chiusura del rapporto. Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dovranno essere osservati anche in seguito a modifica dell'incarico e/o alla cessazione del rapporto di lavoro / collaborazione.

Selezionare tra Lavoro / Collaboratore, a seconda del rapporto esistente tra l'Incaricato che si sta nominando e la Società/Studio che lo nomina.

Luogo e data, _____

Inserire Luogo e data in cui si conferisce tale Incarico

Il Responsabile del Trattamento

_____

L'Incaricato, sottoscrivendo la presente, prende atto di quanto previsto nella presente nomina e dalla normativa vigente ed assume la qualifica di Incaricato del trattamento.
Luogo e data, _____

Inserire Luogo e data in cui l'Incaricato accetta tale Incarico

L'Incaricato del Trattamento

_____

Oggetto: *FAC-SIMILE* DI LETTERA DI NOMINA RESPONSABILI

NOTE METODOLOGICHE
Nel documento di seguito proposto:

- le parti in **nero** sono quelle generalmente idonee per la totalità delle Imprese / degli Studi, in fase di nomina del Responsabile;
- le parti in **blu** sono le sezioni che possono essere differenti, realtà per realtà;
- le parti in ***bordeaux*** e quelle su sfondo grigio sono le note operative, utili per la compilazione, ma da cancellare in sede di definizione della nomina del Responsabile

Carta intestata dell'Azienda / Studio
(soggetto per il quale si sta curando la messa a regime sulla *Privacy*)

Luogo e data, _____

Inserire Luogo e data in cui si consegna il presente incarico

Preg.mo/a Sig / Sig.ra
_____
_____

Inserire i dati anagrafici del Dipendente/Collaboratore cui qui si intende conferire l'incarico di Responsabile

OGGETTO: Nomina del Responsabile al Trattamento dei dati - _____

Specificare l-area di responsabilità. Per esempio: Responsabile Risorse Umane, Responsabile Amministrativo, Responsabile Sistemi Informativi, ecc.

Il / La sottoscritto / a _____
nato / a a _____il _____
Codice Fiscale _____

Qui sopra, occorre riportare i dati anagrafici del Titolare del Trattamento dei dati aziendale / di Studio, che conferisce l'incarico di "Responsabile al trattamento dei dati".

in qualità di Titolare Trattamento dati dell'Azienda / dello Studio _____,

Selezionare tra Azienda e Studio e specificare la denominazione dell'Azienda /Studio. Eventualmente aggiungere, ove il Titolare sia la Società, la locuzione: "nella personale del suo Legale Rappresentante"

vista la normativa in materia di *Privacy* disciplinata dal D.Lgs. n.196/03 Codice in materia di protezione dei dati personali, con la presente nomino:

il Sig. / la Sig.ra _____
nato / a a _____il _____
Codice Fiscale _____

Qui sopra, occorre riportare i dati anagrafici del Responsabile al trattamento dei dati, cui si sta conferendo l'incarico.

Responsabile del Trattamento dei dati nell'ambito delle funzioni che è chiamata a svolgere in relazione al rapporto di lavoro / collaborazione, con le finalità e secondo le modalità stabilite, anche in futuro, dal Titolare e, comunque, in modo lecito e secondo correttezza.

Selezionare tra lavoro / collaborazione in base al rapporto esistente con il soggetto che si sta nominando.

Nell'espletamento del Suo incarico, sarà tenuto a:

- Osservare quanto previsto dal D.Lgs. n.196/03 e le altre disposizioni legislative e regolamentari in materia di riservatezza delle persone osservando i principi di liceità e correttezza.
- Rispettare e far rispettare agli Incaricati quanto disposto dal *Documento Programmatico sulla Sicurezza nel trattamento dei Dati Personali* in vigore e dal *Regolamento Privacy.*

Mantenere questo punto, ove presenti tali documenti, altrimenti depennare

- Definire le procedure di sicurezza da seguire all'interno della propria area di responsabilità per garantire la sicurezza e la correttezza dei dati.
- Promuovere lo sviluppo, la realizzazione ed il mantenimento dei programmi di sicurezza contenuti nel *Documento Programmatico sulla Sicurezza dei Dati Personali.*

Mantenere questo punto ove redatto il DPS, altrimenti depennare

- Scegliere e nominare i Soggetti da incaricare al trattamento dei dati ed impartire loro le istruzioni e l'ambito del trattamento consentito.
- Richiedere al Responsabile dei Servizi informativi, l'attivazione dell'account di posta elettronica e/o il collegamento ad internet per i propri Incaricati, laddove necessario.

Mantenere questo punto ove presente il Responsabile Servizi informativi, oppure adattare rispetto alla specifica struttura aziendale

- Verificare periodicamente la conformità degli incarichi all'attività svolta dai Soggetti Incaricati.

Mantenere questo punto ove presenti Incaricati su cui il Responsabile qui nominato debba effettuare il controllo

- Verificare che per i dati trattati sia stato richiesto ed ottenuto il consenso degli interessati laddove necessario per legge.
- Promuovere lo svolgimento di un continuo programma di formazione degli Incaricati del Trattamento.

Mantenere questo punto ove presenti Incaricati

- Riferire al Titolare del Trattamento in merito a proposte atte a perseguire migliori livelli di sicurezza o ridurre i rischi presenti e sopravvenuti, anche al fine di aggiornare periodicamente il *Documento Programmatico sulla Sicurezza nel Trattamento dei Dati Personali.*

Mantenere quest'ultima parte ove redatto il DPS, altrimenti depennare

Ella dovrà effettuare il trattamento attenendosi ad ogni altra eventuale istruzione impartita dal Titolare del Trattamento, il quale, anche tramite verifiche periodiche, avrà il compito di vigilare sulla puntuale osservanza delle disposizioni impartire e sul rispetto della normativa.

La presente nomina può essere revocata in ogni momento, con effetto immediato e senza obbligo di preavviso. Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dovranno essere osservati anche in seguito a modifica dell'incarico e/o alla cessazione del rapporto di lavoro / collaborazione.

Selezionare tra Lavoro / Collaboratore, a seconda del rapporto esistente tra l'Incaricato che si sta nominando e la Società/Studio che lo nomina

Luogo e data, _____

Inserire Luogo e data in cui si conferisce tale Incarico

Il Titolare del Trattamento

_____

Il Responsabile, sottoscrivendo la presente, prende atto di quanto previsto nella presente nomina e dalla normativa vigente ed assume la qualifica di Responsabile del trattamento.

Luogo e data, _____

Inserire Luogo e data in cui il Responsabile accetta tale Incarico

Il Responsabile del Trattamento

_____

Oggetto: ISTRUZIONI PER LA MODIFICA E LA CUSTODIA DELLE *PASSWORD*

NOTE METODOLOGICHE
Nel documento di seguito proposto:

- le parti in **nero** sono quelle generalmente idonee per la totalità delle imprese interessate alla consegna delle presenti istruzioni;
- le parti in **blu** sono le sezioni che possono essere differenti, realtà per realtà;
- le parti in ***bordeaux*** e quelle su sfondo grigio sono le note operative, utili per la compilazione, ma da cancellare in sede di definizione delle presenti istruzioni.

Carta intestata dell'Azienda / Studio
(soggetto per cui si è redatto il DPS)

Istruzioni sulla custodia della *password*

Luogo e data, _____

Inserire Luogo e data in cui si consegnano le presenti istruzioni

Preg.mo/a Sig/Sig.ra

_____

_____

Inserire i dati anagrafici del Dipendente / Collaboratore cui si consegnano le presenti istruzioni

Il D.Lgs. n.196/03 recante Codice in materia di trattamento dei dati personali, di seguito per brevità denominato *Legge sulla Privacy*, prevede che l'accesso ai programmi *software* e/o agli strumenti elettronici che vengono utilizzati nel normale svolgimento dell'attività lavorativa, sia protetto da una parola chiave (*password*) associata all'identificativo del suo utilizzatore (*user id*), con l'obiettivo di evitare che persone non autorizzate accedano ai dati.
A tal fine, la segretezza della parola chiave è essenziale e dovrà essere garantita attivando le seguenti procedure:

1. Per ogni accesso a *software* cui viene abilitato, avrà una Sua *password*, che dovrà modificare almeno ogni tre mesi;

Segnalare una tempistica eventualmente più ristretta dei tre mesi

2. La parola chiave che imposterà non dovrà contenere riferimenti agevolmente riconducibili a Lei e preferibilmente conterrà lettere maiuscole e minuscole e caratteri speciali (per esempio: *,-,%).

Adattare quest'ultima parte del punto 2, rispetto alla specifica realtà, considerando le possibilità concesse dai software per il cambiamento delle *password*

3. La lunghezza della parola chiave dovrà essere di almeno otto caratteri. Qualora il sistema consenta solo parole chiave più corte, la lunghezza dovrà essere quella massima consentita dal sistema.
4. Sarà tenuto a non comunicare la Sua parola chiave ad altri soggetti, interni o esterni e a non lasciarla in formato intelligibile (post-it, appunti, ...) in evidenza presso la Sua postazione di lavoro;
5. ad ogni cambiamento della *password*, dovrà compilare l'apposito modulo qui allegato, provvedendo a consegnarlo in busta chiusa a_____

Specificare il Soggetto cui occorrerà consegnare la password in busta chiusa. Può essere indicato un cognome e nome o, più opportunamente, un titolo. Per esempio: Responsabile Risorse Umane, Responsabile *Privacy*, ecc.

Il Responsabile _____ potrà fornirLe ogni ulteriore chiarimento ritenesse utile in merito al comportamento da adottare per l'uso di dette *password*.

Segnalare il referente scelto in Azienda / Studio a ciò preposto. Potrebbe essere per esempio: il Responsabile Risorse Umane, il Responsabile Sistemi Informativi, il Responsabile *Privacy*.

Si coglie l'occasione per porgere i più distinti saluti.

Il Titolare / Responsabile

_____

Selezionare a seconda che tale informativa venga consegnata dal Titolare o dal Responsabile. In quest'ultimo caso specificare il ruolo; per esempio Responsabile Risorse Umane, Responsabile Amministrativo,

Per ricevuta

_____

Firma a cura di chi riceve la presente informativa

MODULO PER LA COMUNICAZIONE DELLE VARIAZIONI DELLE *PASSWORD*

Denominazione del *Software*	*Password* precedente	*Password* nuova immessa	Data cambiamento *password*	Firma del Soggetto che ha modificato la *password*

Oggetto: INFORMATIVA DA RACCOGLIERE PRESSO CLIENTI E FORNITORI

Con il provvedimento del Garante del 19/06/08, piccole e medie imprese, professionisti e artigiani possono godere di semplificazioni in ordine a informativa ed esonero dal consenso. Nello specifico:

L'informativa
Il Garante invita a fornire un'informativa "breve", sia oralmente, sia utilizzando gli spazi liberi nel materiale cartaceo e nella corrispondenza normalmente utilizzata per le finalità amministrative e contabili. Questo almeno nella fase iniziale, rinviando poi ad un eventuale testo più articolato, agevolmente consultabile e senza oneri: viene fatto l'esempio del sito *internet*, piuttosto che del messaggio preregistrato accessibile da un numero telefonico gratuito.
Il Garante suggerisce per l'informativa "breve" il seguente testo tipo:

I SUOI DATI PERSONALI
Utilizziamo – anche tramite collaboratori esterni – i dati che la riguardano esclusivamente per nostre finalità amministrative e contabili, anche quando li comunichiamo a terzi. Informazioni dettagliate, anche in ordine al suo diritto di accesso e agli altri diritti, sono riportate su …

Il Consenso
Il Garante ha individuato un nuovo caso di esonero dalla richiesta di consenso all'interessato, stabilendo che le aziende private, che abbiano venduto un prodotto o un servizio, possono utilizzare, senza il consenso, i recapiti di posta cartacea dell'interessato (rimane vietato l'uso del telefono) per inviare materiale pubblicitario, vendere prodotti, fare ricerche di mercato o di comunicazione commerciale. Questo a condizione che l'attività promozionale sia connessa a beni e servizi analoghi a quelli oggetto della vendita originaria, e che l'interessato sia opportunamente informato circa la possibilità di opporsi a questo, in ogni momento e in modo agevole e gratuito.
Ricordiamo che rimangono i casi tipici di esenzione, quali:
- se il trattamento dei dati è svolto per adempiere ad obblighi contrattuali o normativi, o comunque per ordinarie finalità amministrative e contabili;
- se i dati trattati provengono da pubblici registri o elenchi conoscibili da chiunque, oppure sono relativi allo svolgimento di attività economiche dell'interessato.

NOTE METODOLOGICHE
Nel documento di seguito proposto:
- le parti in **nero** sono quelle generalmente idonee per la totalità delle Imprese / degli Studi che compilano la presente informativa;
- le parti in **blu** sono le sezioni che possono essere differenti, realtà per realtà;
- le parti in ***bordeaux*** e quelle su sfondo grigio sono le note operative, utili per la compilazione, ma da cancellare in sede di definizione del contenuto della presente informativa.

"Dichiarazioni di rispetto di quanto previsto dal D.Lgs. n.196/03"

Esempi di Soggetti cui richiedere la presente Dichiarazioni di rispetto di quanto previsto dal D.Lgs. n.196/03:

- **Società di consulenza del lavoro**
- **Dottori Commercialisti**
- **Notai**
- **Consulenti aziendali**
- **Avvocati**
- **Agenti di commercio**
- **Società interinali**
- **Medico preposto alla visita periodica dei dipendenti**
- **Società di consulenza per certificazioni sicurezza e ambiente**
- **Società che effettuano gli interventi su *software***
- **Società che effettuano gli interventi su *hardware***

CARTA INTESTATA
dell'Azienda fornitore / del Consulente /fornitore

ATTESTAZIONE AI SENSI DEL D.LGS. n.196/03

Codice in materia di protezione dei dati personali. Tutela della Privacy

I dati ed i documenti relativi alla Vostra Azienda e al Vostro Personale, sono trattati da _____,

Qui occorre riportare il nome della Società / del Consulente che effettua servizi a favore della Società / dello Studio per il quale si sta predisponendo la documentazione per l'adeguamento alla normativa sulla *Privacy*

Titolare del trattamento dati, o da suoi Responsabili e/o Incaricati, secondo le modalità necessarie, ai fini di adempiere gli obblighi di legge e gli incarichi da Voi conferiti, nel rispetto di quanto previsto dal D.Lgs. n.196/03 e soprattutto nel rispetto dell'obbligo di trattare i dati con sicurezza, riservatezza, liceità.
I dati personali acquisiti:

☐ saranno trattati anche con l'ausilio di mezzi elettronici e/o automatizzati;
☐ saranno trattati esclusivamente a livello cartaceo.

I dati conferiti:

☐ potranno essere oggetto di comunicazione a soggetti terzi (ed in particolare _____)
☐ non potranno essere oggetto di comunicazione a soggetti terzi;
☐ potranno essere oggetto di diffusione.

I dati conferiti:

☐ potranno essere utilizzati per finalità di *marketing*;
☐ non potranno essere utilizzati per finalità di *marketing*.

Detti dati saranno trattati esclusivamente al fine dello svolgimento dell'incarico conferito. Il conferimento dei dati, previa informativa ai sensi dell'art.13, è:

☐ facoltativo;
☐ obbligatorio.

Resta inteso che l'eventuale mancato conferimento del consenso al trattamento, comporterà l'impossibilità di adempimento dell'incarico stesso.
Ai sensi dell'art.7 del D.Lgs. n.196/03 è garantito il diritto di accedere ai propri dati, chiedendone l'aggiornamento, la rettificazione, l'integrazione e, ricorrendone gli estremi, la cancellazione e quant'altro previsto dalla normativa in oggetto, nonché di opporsi in tutto o in parte al loro trattamento.
La sottoscritta Società / Il sottoscritto Consulente certifica di rispettare quanto previsto dal D.Lgs. n.196/03 e di redigere annualmente il DPS.

Mantenere questo richiamo se effettuato effettivamente

Allegati: art.7 e art.13 del D Lgs. n.196/03

Mantenere il richiamo a tali allegati, se allegati alla presente dichiarazione

Luogo e data_____

Inserire Luogo e data in cui si compila la presente dichiarazione

Timbro e firma Azienda / Consulente

_____

Il timbro e la firma saranno dell'Azienda fornitore / del Consulente fornitore

Autorizzazione al trattamento dei dati personali

Con la presente, ai sensi del D.Lgs. n.196/03, essendo a conoscenza delle informazioni di cui all'art.13 e dei diritti ai sensi dell'art.7 della suddetta Legge, esprimo il consenso al trattamento dei dati personali relativi all'Azienda e al nostro Personale ai fini dell'espletamento dell'incarico conferitoVi.

Luogo e data_____

Inserire Luogo e data in cui l'Azienda/lo Studio per il quale si sta predisponendo la documentazione per l'adeguamento alla normativa sulla *Privacy*, acconsentono al trattamento dei dati personali

Timbro e firma Azienda / Studio

_____

Il timbro e la firma saranno dell'Azienda per i quali si sta predisponendo la documentazione per l'adeguamento alla normativa sulla *Privacy*

Autorizzazione al trattamento dei dati sensibili

Con la presente, ai sensi del D.Lgs. n.196/03, essendo a conoscenza delle informazioni di cui all'art.13 e dei diritti ai sensi dell'art.7 della suddetta Legge, esprimo il consenso al trattamento dei dati sensibili relativi all'Azienda e al nostro Personale ai fini dell'espletamento dell'incarico conferitoVi.

Luogo e data_____

Inserire Luogo e data in cui l'Azienda / lo Studio per il quale si sta predisponendo la documentazione per l'adeguamento alla normativa sulla *Privacy*, acconsentono al trattamento dei dati personali

Timbro e firma Azienda / Studio

_____

Il timbro e la firma saranno dell'Azienda per i quali si sta predisponendo la documentazione per l'adeguamento alla normativa sulla *Privacy*

Autorizzazione al trattamento dei dati <u>per finalità di *marketing*</u>

Con la presente, ai sensi del D.Lgs. n.196/03, essendo a conoscenza delle informazioni di cui all'art.13 e dei diritti ai sensi dell'art.7 della suddetta Legge, esprimo il consenso al trattamento dei dati per finalità di *marketing*, relativi all'Azienda e al nostro Personale ai fini dell'espletamento dell'incarico conferitoVi.

Luogo e data_____

Inserire Luogo e data in cui l'Azienda/lo Studio per il quale si sta predisponendo la documentazione per l'adeguamento alla normativa sulla P*rivacy*, acconsentono al trattamento dei dati personali

Timbro e firma Azienda / Studio

_____

Il timbro e la firma saranno dell'Azienda per i quali si sta predisponendo la documentazione per l'adeguamento alla normativa sulla *Privacy*