Regolamento Europeo 2016/679
Piano di Adeguamento per il Data Protection
Migrazione sistema Dlg.196/03 alla DPGR-EU

MSP Manuale del Sistema Privacy e Data Protection
Già Piano di adeguamento ai sensi del Dlg 318/96

SISTEMA PER IL TRATTAMENTO DELLE INFORMAZIONI PERSONALI
(VERSIONE LEGACY SUPERATA DA DATA PROTECTION 2016)

EDIZIONE ABROGATA DEL 2012-14

Riferimento : MSI196 (Manuale del Sistema Informativo – Abrogato DPS)
Versione : 3.6 - Mar 2012
Aggiornamento : 3.6bis - Nov 2014
Ultima revisione modulo : 4.0 Nov 2014

Documento (SOSTITUITO DAL DISCLIPLINARE INTERNO DALLA EDIZIONE 2012-13)

Manuale del Sistema Informativo applicato in conformità al Disciplinare Tecnico Allegato B del Codice per il trattamento dei dati personali.

Il MANUALE del SISTEMA INFORMATIVO, nel seguito **MSI**, raccoglie e regola l'insieme di prassi, di procedure e di istruzioni operative che riguardano gli aspetti di controllo tecnologico informatico e telematico adottati dalla nostra società per adeguarsi al Disciplinare Tecnico dell'Allegato B del Codice della Privacy. Il **MSI** è parte integrante del **MSP** della Società. Il presente documento ha titolo di formazione ai sensi della regola 19.6 del Disciplinare Tecnico in Materia di Misure Minime di Sicurezza (Allegato B al Codice Privacy)

Dichiarazione del Titolare del trattamento

La nostra Società tratta tutti i dati personali e recepisce i principi di necessità di cui all'Art. 1 del codice del Garante della Privacy; adotta pertanto tutte le misure **tecnologicamente aggiornate e sostenibili** nel trattamento delle informazioni in formato elettronico ritenendo di dover agire preventivamente nel futuro qualora nuove attività investano l'ambito di applicazione del Decreto Legge 196/03.

INFORMAZIONE E FORMAZIONE ALLE PARTNERSHIPS /CONTITOLARI /FORNITORI ICT (Art. 164)

Il **MSI** viene divulgato agli incaricati e tutti i partners tecnologici a scopo di istruzione e consultazione per quanto di propria competenza e campo di applicazione in relazione alle specifiche istruzioni operative. L'Amministratore del Sistema Informativo e/o il Responsabile del trattamento forma/no gli incaricati e informano i partners affinché siano consapevoli delle procedure di misure di sicurezza in ambito privacy e data protection.

Il MSI è anche lo strumento di periodico aggiornamento per il piano di formazione previsto dal Disciplinare Tecnico dell'Allegato B del Codice della Privacy e rappresenta la politica di sicurezza di riferimento per i fornitori esterni di Harware e Software. Come da prescrizioni del Codice agli *out-sourcers* del sistema informativo sono trasmesse copie del MSI perché conoscano le politiche della Società in materia di protezione dei dati personali.

Aggiornamento e rintracciabilità

Il **MSI** viene conservato dopo approvazione del Titolare Del Trattamento cosi come definito nei documenti di Delega in allegato a tutti i soggetti del Sistema Privacy.

Qualunque revisione periodica al **MSI**, o ad una parte di esso, ne crea versioni successive mantenendo riferimento agli indici dei documenti **Index2012-13**. Le revisioni successive del MSI sono contro firmate dal Responsabile del trattamento e dall'Amministratore di Sistema (se presente)

Titolare del trattamento
R&S MANAGEMENT S.r.l.
l'amministratore unico
Dott.ssa Serena Borelli
Serena Borelli
.....

ADS / Responsabile trattamento
Ryabokhin Yaroslav
pour Bell

Regolamento Europeo 2016/679
Piano di Adeguamento per il Data Protection
Migrazione sistema Dlg.196/03 alla DPGR-EU

MSP Manuale del Sistema Privacy e Data Protection
Già Piano di adeguamento ai sensi del Dlg 318/96

Redazione e responsabilità
La redazione del MSI è curata congiuntamente dal Responsabile del Trattamento dei dati e dell'Amm.re di Sistema (se persona diversa o in out-sourcing). Formale incarico e delega è stata assegnata agli interessati designati dal Titolare del trattamento (Artt. 29 e 30 - vedi Allegati al PA/196 e).

MANUALE DEL SISTEMA INFORMATIVO

eX LEGE : ALLEGATO B - Codice in Materia di Privacy
DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA
(Artt. da 33 a 36 del codice)

Sommario documento

DEFINIZIONI

MSP	Manuale del Sistema Privacy
POST/BIOS	Sistema di configurazione permanente per controllo di accensione di un elaboratore elettronico
LAN	Local Area Network
ADS	: Amministratore dei Sistemi Informativi ovvero persona interna alla società o in out-sourcing con delega scritta ad operare per la stesura del MSI. Amm SI e Responsabile del Trattamento possono essere la stessa persona ed in questo caso
FDP	Banche dati, repertori e documenti in formato elettronico sono di seguito riferiti come File con Dati Personali ovvero **FDP**
SI	L'insieme degli apparati informatici saranno di seguito riportati coma **Sistema Informativo** ovvero **SI**

1. PREAMBOLO e DESCRIZIONE GENERALE DEL SISTEMA
Il presente documento rappresenta materiale di formazione per gli Incaricati che possono richiederne la consultazione in qualunque momento. Dove istruzioni impartite facciano riferimento a documenti o registrazioni non pubbliche, agli incaricati vengono fornite istruzioni per iscritto relative alle modalità procedurali che li riguardano. Gli incaricati che firmano il documento di delega e il foglio di nomina sono al corrente dei contenuti di questo manuale per quanto di loro competenza.
Il **MSI** rappresenta punto di riferimento comune per le mansioni di Responsabile del trattamento, Amministratore **SI** (se persona diversa o consulente in out-sourcing) e del personale (ovvero *Incaricati*); tutti si attengono alle istruzioni e le direttive contenute in questo documento che riflette la politica della Società in materia di privacy.

La nostra Società dispone di un numero inventariato di elaboratori e dispositivi elettronici. Indipendentemente dalla distribuzione e delle diverse locazioni (locali o remote) delle stazioni di lavoro, tutti gli elaboratori fanno capo ad un Network aziendale il cui accesso prevede l'uso di una o più aree Server.
La fornitura dei dispositivi elettronici e del software di gestione data-bank sono garantiti dai fornitori informatici che hanno firmato un attestato di conformità. Tutti gli interventi manutentivi delle società esterne attestate sono comunque svolti senza che i loro operatori siano mai a conoscenza delle credenziali del Sistema di Autenticazione e Autorizzazione (vedi Istruzioni operative punti **3.1.A** e **3.3.A** del MSI)

Il network informatico interno a uffici di una stessa filiale (**LAN**) consta di computer inventariati in registri locali che sono periodicamente aggiornati dai responsabili (**EL4/4**). Questi computer sono collegati tramite rete *Ethernet* e le credenziali di tutti gli utenti che accedono al sistema sono centralizzate in una stazione Server. Tutti i client sono anche forniti di controllo di accensione prima di avere accesso alle funzioni della rete aziendale. I Server dati prevedono la gestione delle unità di backup per le copie di sicurezza. Il network prevede altri dispositivi di scanning, e/o cattura immagini per acquisizioni in formato digitale ma solo via abilitazione delle porte USB.

QUADRO 1A: NOTE ADDIZIONALI DI AGGIORNAMENTO (DOTAZIONE INFORMATICA E FINALITA')

……

CABINET DEL SERVERs SONO DOTATI DI SERRAMENTO ALLA PANNELLATURA. CHIAVE DI COPIA E' CONSERVATA IN CONTENITORE ALTER LOCO IN ZONA AD ACCESSO CONTROLLATO E COMUNQUE, SE SPOSTATO, IN AREA NON PUBBLICA.

……

SCANNER E DISPOSITIVI DI ACQUISIZIONE ESTERNI VIA USB SONO CONTROLLATI VIA CREDENZIALE DEL POST DI OGNI PC (CLIENT E/O SERVER)
LE FUNZIONI DI ACCENSIONE DI UN PC DA MEDIA ESTERNI SONO INIBITE A LIVELLO DI BIOS PER TUTTE LE STAZIONI DESKTOP DELLA LAN (***OP1MSI***)

Tutte le misure si intendo applicate anche per filiali, sedi distaccate o data Center remoti in regime di Housing o Hosting

Resp. / Amm.SI

……

Istruzioni Quadro 3A
Compilare facoltativamente in stampatello per completare o aggiornare informazioni non presenti nei documenti di inventario. Se non necessario barrare comunque e apporre firma)

3. Trattamento con strumenti elettronici
La nostra società è dotata di strumenti di elaborazione informatici di cui in documento allegato **EL2/3** redatto e aggiornato dal Responsabile con l'Amministratore di Sistema (se altra persona o out-sourcing di consulenza tecnica)
Indipendentemente dal tipo di trattamento la Società mantiene aggiornato e registrato questo inventario secondo cadenze di tempo adeguate al tipo di trattamento.
Tutti gli strumenti di elaborazione o dispositivi potenzialmente connessi in LAN sono considerati come potenzialmente in grado di accedere a dati personali (inventariati in **EL4/4**) residenti su stazioni server o volume dedicati dentro la LAN.
Le informative di cui al documentale attuative possono essere divulgate elettronicamente via web se la Società lo adotterà su un proprio sito di riferimento.

QUADRO 3A: DESCRIZIONE SUPPLEMENTARE DELLA DOTAZIONE INFORMATICA E DELLE FINALITA' DI UTILIZZO RISPETTO AL TRATTAMENTO DI DATI PERSONALI

TUTTI I COMPUTER NEI LOCALI DI UFFICIO SONO ACCESSIBILI SOLO DAL PERSONALE TRAMITE AUTENTICAZIONE E AUTORIZZAZIONE. STAZIONI EVENTUALMENTE NON AGGIORNATE HANNO ALMENO IL CONTROLLO DI AUTENTICAZIONE
LE STAZIONI DI SEGRETERIA POTENZIALMENTE VISIBILI SUL DESK DELL'ACCOGLIENZA PER I SERVIZI CLIENTI E CORTESIA, SONO COMUNQUE INSTALLATI IN MODO CHE LO SCHERMO RISPETTI I CRITERI DI NON VISIBILITA' PER LA CLIENTELA E I VISITATORI
DUE STANZE DEDICATE E INDICATE DA SEGNALETICA SONO RISERVATE ALLO STOCCAGGIO E AL DEPOSITO DI VECCHI ARCHIVI CARTACEI
Tutte le misure si intendo applicate anche per filiani, centri distaccati o data senter remoti in regime di Housing o Hosting

Resp. / Amm.SI

……

Regolamento Europeo 2016/679
Piano di Adeguamento per il Data Protection
Migrazione sistema Dlg.196/03 alla DPGR-EU

MSP Manuale del Sistema Privacy e Data Protection
Già Piano di adeguamento ai sensi del Dlg 318/96

Istruzioni Quadro 3A
Compilare facoltativamente in stampatello per completare o aggiornare informazioni non presenti nei documenti di inventario. Se non necessario barrare comunque e apporre le firma)

Nota di pubblicazione per adeguamento e/ aggiornamento
Riedizioni o modifiche all'assetto e/o alle procedure del Sistema Informativo, non comportano la modifica del presente MSI. Separato allegato verrà aggiunto a compendio della documentazione di Sistema e farà riferimento a questo punto del MSI con data e firma del Amm. Si ovvero Responsabile

3.1 - Sistema di autenticazione informatica
La società ha classificato e regolato l'accesso agli elaboratori elettronici così che per ogni stazione di lavoro che lo richieda all'interno della filiale esista un vincolo di autenticazione (vedi documento : EL3/3)

L'Autenticazione riguarda l'uso controllato di stazioni di elaborazione dati e/o terminali sulla base di una parola chiave legata alla stessa stazione in formato *credenziale identificativa* con uso di *codice di accesso (ovvero PassWord)*. Gli incaricati possono, a seconda delle loro attività di trattamento e responsabilità di funzione aziendale, godere di più credenziali che sono loro comunicate e assegnate dal Responsabile del trattamento e/o Amministratore SI (se altra persona o in out-sourcing)

La credenziale di accensione (***autenticazione***) viene resa nota alle sole persone Incaricate, come da elenco in delega **SOP3/3** . Agli incaricati sono impartite istruzioni comportamentali pertinenti le modalità di uso delle credenziali; quindi gli incaricati con la firma delle deleghe e delle relative istruzioni operative contenute nel foglio di nomina, si obbligano formalmente alla massima diligenza.
Le parole chiave (o codici di utilizzo) utilizzate per l'autenticazione hanno un numero di almeno 8 caratteri tranne i casi in cui il dispositivo e/o periferica utilizzata non lo permetta e sono rinnovate secondo un calendario di scadenze deciso dal Responsabile conforme alle prescrizioni di legge.

3.1.A – Istruzione operativa per registrazione credenziali di Autenticazione
Il Responsabile convoca l'Amministratore di Sistema (ovvero fornitore esterno per la consulenza del Sistema Informativo), il quale accede alle funzioni di configurazione del sistema LAN tramite credenziali di autenticazione fornite dal Responsabile.
Quando necessario l'Amministrazione di Sistema (o consulente sistemista) porta al menu di registrazione del codice POST/BIOS il Responsabile; quest'ultimo, può inserire i codici di Autenticazione precedentemente decisi e peculiari di ogni Computer. Questa operazione sarà quindi ripetuta con cadenza circa semestrale (salvo diverse indicazioni nel documento del piano di adeguamento degli anni precedenti (ex **PA/196 abrogato 2010**).

QUADRO 3.1A: DESCRIZIONE SUPPLEMENTARE SULLA GESTIONE DELLE CREDENZIALI PER LA AUTENTICAZIONE

……
……
REGISTRAZIONE E CONDUZIONE SEGRETA DEI CODICI DI AUTENTICAZIONE E AUTORIZZAZIONE DEL SISTEMA INFORMATIVO SONO FORMALIZZATE DAL DOCUMENTO **OP3/4**
……
……
Tutte le misure si intendo applicate anche per filiani, centri distaccati o data senter remoti in regime di Housing o Hosting

Resp. / Amm.SI

……

Istruzioni Quadro 3A
Compilare facoltativamente in stampatello per completare o aggiornare informazioni non presenti nei documenti di inventario. Se non necessario barrare comunque e apporre firma)

Nota di pubblicazione per adeguamento e/ aggiornamento
Riedizioni o modifiche all'assetto e/o alle procedure del Sistema Informativo, non comportano la modifica del presente MSI. Separato allegato verrà aggiunto a compendio della documentazione di Sistema e farà riferimento a questo punto del MSI con data e firma del Amm. Si ovvero Responsabile

3.2 - Scadenze e attribuzioni credenziali
A meno di finalità per gestione tecnico-amministrativa, le coppie di "*identificazione*" e "*parola chiave*" non sono mai attribuite simultaneamente e sono rinnovate dall'Amministratore SI con cadenza almeno semestrale.

Questa ultima evenienza comporta la riedizione del documento di registro corrispondente **EL4/4**. Una riedizione del documento di credenziali è stilata anche nel caso di modifiche in organigramma per la defezione o l'acquisizione di nuovi Incaricati.

Il Responsabile del Trattamento con l'Amministratore SI (se presente o in out-sourcing) curano le direttive di custodia delle copie dei documenti delle credenziali in modo da garantirne la massima segretezza anche nel caso di mancanza di uno o più incaricati.

Due registri sono mantenuti in aggiornamento per la identificazione e l'etichettatura dei luoghi, degli arredamenti a serramento e/o accesso controllato (vedi **OP3/3**)

QUADRO 3.2A: DESCRIZIONE SUPPLEMENTARE SULLA GESTIONE DELLE AREE E DEI DISPOSITIVI DI CONTROLLO DI ACCESSO

……
……
SE PRESENTE, IL SISTEMA DI ALLARME CON O SENZA VIDEO-SORVEGLIANZA A REGISTRAZIONE E' REGISTRATO NELLA PROCEDURA DI INVENTARIO RESA PUBBLICA COME INFORMATIVA PUBBLICA
……

NESSUN DISPOSITIVO DI RILEVAZIONE BIOMETRIA E' UTILIZZATO PER IL PERSONALE E PER LA CLIENTELA
……

……

Resp. / Amm.SI

……

Istruzioni Quadro 3.2A
Compilare facoltativamente in stampatello per completare o aggiornare informazioni non presenti nei documenti di inventario. Se non necessario barrare comunque e apporre firma)

3.3. - Sistema di autorizzazione
La società ha classificato e individuato l'accesso ai repertori di banche dati e documenti elettronici che lo richiedano (FDP**); all'interno del sito esiste un vincolo di autorizzazione (vedi documento :** EL3/3**)**

La **Autorizzazione** riguarda l'uso controllato di stazioni di elaborazione dati e/o terminali sulla base di una parola chiave legata a ***credenziale identificativa (user)*** e ***codice di accesso (ovvero PW)***. La combinazione delle credenziali accede all'uso del Sistema Operativo del computer, quindi delle sue risorse in ragione del profilo utente riconosciuto.

L'incaricato dotato di credenziali di autorizzazione è tenuto a lasciare incustodita la propria stazione di lavoro solo dopo aver restituito il controllo della stazione al sistema di controllo di accesso per l'Autorizzazione o al salva schermo del Sistema Operativo (se disponibile)

La verifica del sistema di autorizzazione viene comunque redatta in cadenza circa annuale, ossia in corrispondenza della riedizione del **DPS** della Società.

3.3A – Istruzione operativa per registrazione credenziali di Autorizzazione
Il Responsabile convoca l'Amministratore di Sistema (e o l'intervento tecnico esterno del consulente sistemista), il quale accede alle funzioni di configurazione del sistema LAN tramite credenziali di autenticazione fornite dal Responsabile.

Per registrare le credenziali di autorizzazione sul Server (se presente) l'Amministratore di SI o consulente Sistemista porta la finestra di configurazione del Codice Segreto alla portata di ogni singolo incaricato affiancandolo per le informazioni pubbliche (*Username*) e lasciando il controllo della tastiera all'Incaricato che inserisce il proprio codice segreto corrispondente a quello contenuto nella busta consegnata al Responsabile.

QUADRO 3.3A: DESCRIZIONE SUPPLEMENTARE SULLA GESTIONE DELLE CREDENZIALI PER LA AUTORIZZAZIONE DEGLI INCARICATI DEL TRATTAMENTO (laddove applicabile)

……

LE STAZIONI DI LAVORO LASCIATE INCUSTODITE SONO PROTETTE DAL SISTEMA DI SALVA SCHERMO DEL COMPUTER CHE RESTITUISCE IL CONTROLLO SOLO DOPO PROCEDURA DI AUTORIZZAZIONE A MEZZO CREDENZIALI ATTRIBUITE PERSONALMENTE (***OP3/4, OP1MSI***)

……

NELLE STAZIONI CON SISTEMA OPERATIVO WINDOWS 98 O PRECEDENTE, I PC SONO SPENTI E L'ACCESSO AL SISTEMA SFRUTTA COMUNQUE IL LIVELLO DI AUTENTICAZIONE ALLA ACCENZIONE

……

Resp. / Amm.SI DPO

……

Istruzioni Quadro 3.3A
Compilare facoltativamente in stampatello per completare o aggiornare informazioni non presenti nei documenti di inventario. Se non necessario barrare comunque e apporre firma)

3.4 – Criteri generali di mantenimento delle Autenticazione e Autorizzazione
Le disposizioni sul sistema di autenticazione e quelle sul sistema di autorizzazione di cui ai precedenti punti del MSI non vengono seguite per eventuali informazioni di trattamenti dati personali destinati alla diffusione esterna alla società, per dati che non rientrano nella analisi dei rischi (Punto 3. PA/196).

4.0 - Altre misure di sicurezza
Dove applicabile, è possibile creare delle liste di incaricati omogenee per incarico anche su più stazioni di lavoro
Se individuati in inventario, gli elaboratori del Sistema Informativo coinvolti e/o potenzialmente esposti ad intrusione sono soggetti a installazione e configurazione di Programmi Antivirus e Firewall (registro **EL4/5)**

Nei casi di dati "***sensibili***" anche misure di **cifratura** per le copie di sicurezza sono adottate a cura del Responsabile e/o dell'Amministratore di SI

Conformità : [… omissis-…] " rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale".

In relazione alla conformità sopra citata, l'Amm.re SI cura le cadenze di aggiornamento istruendo gli incaricati in caso di modifiche alle procedure di sistema. Nei casi di out-source la nostra società provvede all'a acquisto di software di terza parte per assolvere alle procedure di cifratura necessarie.

QUADRO 4.0: DESCRIZIONE SUPPLEMENTARE SUI CRITERI E SULLE MODALITA' DI PROTEZIONE E CIFRATURA DELLE COPIE DI SICUREZZA PER DISASTER RECOVERY

……

……

……

……

……

Resp. / Amm.SI

……

Istruzioni Quadro 4A
Compilare facoltativamente in stampatello per completare o aggiornare informazioni non presenti nei documenti di inventario. Se non necessario barrare comunque e apporre firma)

4.1 – Aggiornamenti protezione e vulnerabilità
Gli aggiornamenti periodici dei programmi di cui al *punto 4.0* sono gestiti dall'Amm. SI che mantiene attive e verificabili le politiche di licenza dei prodotti software e conosce le scadenze di rinnovo e di aggiornamento.
(In assenza di un Amm.SI il Responsabile prende in consegna queste attività).

Il modello di inventario EL4/5 riporta elenco aggiornato dei programmi e delle metodologie software utilizzare con estremi di licenza e scadenze.

QUADRO 4.1: DESCRIZIONE SUPPLEMENTARE SUI CRITERI E SULLE MODALITA' DI PROTEZIONE DI VULNERABILITA'

……

……

……

Resp. / Amm.SI

……

4.2 – Copie di Sicurezza e misure anti-deperimento
Per garantire la applicabilità degli dei diritti degli Interessati di cui agli Artt. 3,5, 7 e 8 del codice, la Società cura un inventario di dispositivi e procedure di Backup di Sistema curati dai Responsabili e dall'Amm. SI (se presente).

Nel caso delle banche dati individuate nell'elenco del registro **EL4/4** i dati di cui sono effettuate copie di sicurezza sono registrati in dispositivi protetti da credenziale di autenticazione e autorizzazione (vedi i punti 3.0) e i supporti informativi di informazione sono conservati in luoghi sicuri e/o contenitore di sicurezza.

QUADRO 4.2: DESCRIZIONE SUPPLEMENTARE SUI CRITERI E SULLE PROCEDURE DI COPIA DI SICUREZZA E CIFRATURA DI PROTEZIONE

……

LE COPIE DI BACKUP SONO TENUTE IN LUOGO SICURO E DIVERSO DALLA LOCAZIONE DELLA STAZIONE DI LAVORO CHE LE HA PRODOTTE

……

……

Tutte le misure si intendo applicate anche per filiani, centri distaccati o data senter remoti in regime di Housing o Hosting

Resp. / Amm.SI

……

4.3 – Frequenza e cadenza copie di sicurezza
Le procedure per le copie di Sicurezza dei dati sono effettuate con cadenza variabile a seconda della discrezionalità del Amm. SI e/ e dei Responsabili; per i repertori identificati come **FDP** ai sensi del Codice, hanno comunque cadenza almeno settimanale.

L'Amm.SI si può avvalere di strumenti software per la programmazione automatica delle procedure per le copie di Sicurezza e deve informare almeno una persona "Incaricato", tra quelli delegati, che conosca la stessa procedura e la possa gestire in situazioni di emergenza e/o di malfunzionamento del Sistema Informativo (vedi **OP1/1, EL4/4**).

Le copie di Sicurezza riguardano anche le credenziali degli incaricati che le conservano in busta chiusa e in luogo sicuro consegnandole al proprio responsabile (vedi **Quadro 11.2° PA196**).

L'Amministratore SI conosce il luogo sicuro dove poter accedere alle credenziali di un Incaricato in caso di emergenza. Egli è autorizzato dal Titolare ad usare le credenziali di un incaricato che sia impossibilitato o non presente.

QUADRO 4.3: DESCRIZIONE SUPPLEMENTARE SUI CRITERI E SULLE CADENZE DELLE PROCEDURE DI COPIA DI SICUREZZA

……

……

QUANDO LA PROCEDURA DI COPIA DI SICUREZZA ALL'ESTERNO DELLE MEMORIE DI SISTEMA LAN PREVEDANO UNA CIFRATURA IL SEME O CHIAVE DI PROTEZIONE VIENE REGISTRATA IN **OP1/1**

……

FREQUENZA LOCALI DEL NETWORK INTRAMURALE CIRCA-GIORNALIERE (SIA MANUALE CHE AUTOMATICA)

……

Resp. / Amm.SI

……

5.0 - Documento programmatico sulla sicurezza

La nostra società si è dotata di un Documento Programmatico della Sicurezza (**DPS**) che consta dei documenti di indice, di delega ovvero incarico, di Manuale del Sistema Informativo e di tutti gli allegati.

La parte pubblica della documentazione di Sistema è disponibile e visionabile da chiunque possa esigerlo per competenza e delega, mentre registri, incarichi di delega e inventari segreti sono conservati in luogo sicuro.

5.1 – Rinnovi e aggiornamenti

Il Documento di Sistema è in continuo aggiornamento in ogni sua parte a seconda delle prescrizioni per le diverse aree di applicabilità ed è curato a seconda degli incarichi assegnati dalle persone ovvero funzioni aziendali competenti.

5.1 – DPS contenuti

Le parti del DPS sono strutturate in modo da prevedere e soddisfare i contenuti minimi previsti dal Codice in materia di privacy che sono di seguito riassunti per verifica e controlli ai sensi Art. 180 comma 2 del Codice

- *Elenco dei trattamenti di dati personali*
- *Distribuzione dei compiti e delle responsabilità implicate nel trattamento dei dati;*
- *Analisi dei rischi potenziali impliciti del trattamento dei dati;*
- *Misure adottate per garantire l'integrità e la disponibilità dei dati,*
- *Protezione e definizione di aree e locali, rilevanti ai fini della loro custodia e accessibilità;*
- *Descrizione dei criteri e delle modalità delle misure anti-danneggiamento ovvero anti-deperimento*
  Piano di interventi formativi degli incaricati del trattamento,
- *Programmazione di interventi formativi per cambiamenti di mansioni, o nuovi strumenti e/o dispositivi tecnologici*
- *Descrizione dei criteri adottati misure minime di sicurezza affidate all'esterno della società*

- *Criteri adottati per la cifratura o per la separazione di dati diffusi all'esterno dagli altri dati personali dell'interessato.*

Le aree di interesse costituiscono anche sommario dei contenuti di formazione. Le aree sono trattate interamente a scopo di formazione e hanno riscontro formale nel nel DPS solo se applicabili al tipo di trattamento e di funzioni aziendali della società.

6.0 - Ulteriori misure in caso di trattamento di dati sensibili o giudiziari
Misure addizionali per eventualità di trattamenti anche transitori nonprevisti dalle normali attività della società al tempo della stesura dell'ultima revisione del Manuale del Sistema Informativo, sono curate dal Responsabile e dall'Amministratore di Sistema (ove presente) e sono regolate nella istruzione Operativa ***OP1MSI***

7.0 - Misure di tutela e garanzia
Se necessario la Società si riserva di acquisire consulenze in regime di Out-sourcing per la politica di sicurezza del trattamento di dati personali. In questa circostanza, i soggetti di partnership sono resi parte del sistema **DPS** operante e sono delegati per iscritto sulla responsabilità di rispettare tutte le politiche della società in materia di Privacy.

I soggetti di terza parte sono informati anche delle conformità ai sensi del Dlg 196/03 e dei suoi allegati incluso Disciplinare tecnico per mantenere coerenza e allineamento con le attività svolte dal Titolare e del Responsabile del Trattamento (vedi Informativa di cui al documento **SOP1/3, SOP4/3 e SOP5/3**).

Il Titolare del trattamento riferisce nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione del documento programmatico sulla sicurezza.

8.0 - Trattamenti senza l'ausilio di strumenti elettronici

Il Titolare del trattamento, il responsabile, ove designato, e dell'incaricato, seguono tutte le politiche di prevenzione e sicurezza adottate per il trattamento de dati con strumenti elettronici anche nel caso di trattamento con strumenti diversi da quelli elettronici.

Tutti i documenti di incarico e delega, manuali e istruzioni operative concernenti le misure di sicurezza per il trattamento dei dati personali sono di piena attuazione sia per dati su supporto elettronico/digitale che su cartaceo.

Specifiche istruzioni sono impartite agli incaricati in merito a :

- *Controllo ed alla custodia,*
- *Analisi del ciclo necessario allo svolgimento delle operazioni di trattamento,*
- *Aggiornamento periodico con cadenza almeno annuale lista degli incaricati,*
- *Confinamento del trattamento di atti e documenti,*
- *Controllo e criteri di custodia da parte di incaricati fino alla restituzione per operazioni affidate ad altri o salvate,*
- *Criteri di comportamento e cautela degli incaricati dopo l'orario di chiusura (identificazione e registro).*

Istruzione operativa e descrizione delle aree ad accesso controllato con inventario arredamento ignifugo a serramento in **OP3_3.**