MANUALE DI DATA PROTECTION

IL MANUALE DI DATA PROTECTION AL FINE DI OTTEMPERARE ALLE DISPOSIZIONI DEL REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO DEL 27 APRILE 2016

Società	FERRARI MECCANICA S.P.A.
Comune	MILANO (MI)
Indirizzo	PIAZZA DELLA REPUBBLICA 30
Descrizione dell'attività svolta	PRODUZIONE E COMMERCIO IMBALLAGGI METALLICI

S E Z I O N I

1- PREMESSE

"Chiunque ha diritto alla protezione dei dati personali che lo riguardano"

Questa è la base del Regolamento Europeo 2016/679 che disciplina la normativa in materia di tutela della protezione dei dati.

Il Regolamento garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Per garantire che i rischi di distruzione o perdita, anche accidentale, dei dati personali siano ridotti al minimo, devono essere adottate idonee e preventive misure di sicurezza quali:

a) autenticazione informatica;

b) adozione di procedure di gestione delle credenziali;

c) utilizzazione di un sistema di autorizzazione;

d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;

e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;

f) adozione di procedure per la custodia di copie di sicurezza, del ripristino della disponibilità dei dati e dei sistemi;

g) tenuta di un aggiornato manuale di data protection;

h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Il **MANUALE DI DATA PROTECTION** è redatto per definire le misure minime di sicurezza che debbono essere adottate in via preventiva dal soggetto responsabile, in conformità a quanto previsto dal Regolamento Europeo 2016/679.

Altresì sono riportate le misure adottate per prevenire e 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, intendendosi per misure di sicurezza il complesso degli accorgimenti tecnici, informatici, organizzativi, logistici e procedurali di sicurezza.

Area di applicazione

Il **MANUALE DI DATA PROTECTION** definisce le politiche e gli standard di sicurezza in merito al trattamento dei dati personali, individuando le linee guida generali, le azioni e le misure per il trattamento dei dati personali in condizione di sicurezza.

Documento Programmatico sulla Sicurezza

I dati:

- Personali
- Identificativi
- Sensibili
- Genetici
- Biometrici

Devono essere trattati con:

- Strumenti elettronici di elaborazione ed altri strumenti cartacei di elaborazione

Il Documento Programmatico sulla Sicurezza deve essere conosciuto ed applicato da tutti gli incaricati nominati.

MANUALE DI DATA PROTECTION informazioni base:

E' previsto che il **MANUALE DI DATA PROTECTION** sia definito con un contenuto informativo base che preveda:

- elenco dei trattamenti di dati personali;
- distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- analisi dei rischi che incombono sui dati;
- misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione, danneggiamento o cancellazione;
- previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi e dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
- descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
- modus operandi per i dati personali idonei a rivelare lo stato di salute e la vita sessuale (dati sensibili), l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

In conclusione

Le misure individuate perseguono l'obiettivo di ridurre al minimo, con riferimento alla tipologia dei dati trattati, i rischi di distruzione o perdita degli stessi, nonché i rischi di accesso non autorizzato, il trattamento non consentito o non conforme alle finalità di raccolta.

In tal senso il **MANUALE DI DATA PROTECTION** individua soggetti, compiti e responsabilità in materia di sicurezza dei trattamenti, descrivendo le modalità per l'analisi e la valutazione dei rischi, nonché le misure necessarie per ridurre tali rischi al minimo.
In termini operativi il **MANUALE DI DATA PROTECTION** individua non soltanto la protezione del patrimonio informativo da accessi non autorizzati e rischi di cancellazione, distruzione o perdita di dati, ma anche la limitazione degli effetti causati dall'eventuale occorrenza di tali cause.

La stesura del **MANUALE DI DATA PROTECTION** rispecchia le seguenti linee guida:

a) analisi dello stato dell'organizzazione attraverso l'identificazione e distinzione delle responsabilità delle figure soggettive coinvolte nel trattamento;

b) l'identificazione;

c) l'inventario e l'analisi dell'hardware, del software e delle banche dati;

d) l'individuazione e la valutazione del rischio;

e) l'individuazione delle misure preventive e correttive;

f) l'individuazione di istruzioni agli incaricati e la previsione di un programma formativo;

g) la gestione da parte di terzi delle banche dati aziendali.

2- Definizioni normative

Terminologia di primaria importanza da conoscere per una corretta gestione del GDPR

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

Raccolta: atto del raccogliere. Radunare, mettere insieme, concentrare in un punto. (Fonte: Vocabolario della Lingua Italiana Zingarelli)

Registrazione: operazione, effetto del registrare. Scrivere in un registro. Dicasi registro documento pubblico, spesso in forma di libro o fascicolo, in cui si annotano atti giuridicamente rilevanti concernenti beni e persone fisiche o giuridiche al fine di assicurare loro pubblicità verso i terzi e valore probatorio. (Fonte: Vocabolario della Lingua Italiana Zingarelli)

Organizzazione: modo, atto ed effetto dell'organizzare. Ordinare, disporre, preparare. (Fonte: Vocabolario della Lingua Italiana Zingarelli)

Conservazione: atto, modo, effetto del conservare o del conservarsi. Custodire, possedere ancora dopo un lungo periodo di tempo. (Fonte: Vocabolario della Lingua Italiana Zingarelli)

Consultazione: atto, modo, effetto del consultare o del consultarsi. Interrogare per avere un parere, un consiglio, un'informazione e simili. Esaminare con cura.
(Fonte: Vocabolario della Lingua Italiana Zingarelli)

Elaborazione: atto, effetto dell'elaborare. Eseguire, formare, comporre o preparare qualcosa con grande applicazione, diligenza e studio dei particolari, avendo cura di svolgerne, svilupparne, trasformarne o perfezionarne gli elementi di fondo, i dati caratterizzanti e simili.
(Fonte: Vocabolario della Lingua Italiana Zingarelli)

Modificazione: atto, effetto del modificare. Mutare in parte o completamente, cambiare.
(Fonte: Vocabolario della Lingua Italiana Zingarelli)

Selezione: scelta degli elementi migliori o più adatti a un determinato fine. Operazione consistente nell'estrarre da una sequenza di dati quelli contrassegnati da certi indicativi.
(Fonte: Vocabolario della Lingua Italiana Zingarelli)

Estrazione: atto, effetto dell'estrarre. Trarre fuori da qualcosa.
(Fonte: Vocabolario della Lingua Italiana Zingarelli)

Raffronto: atto, effetto del raffrontare. Paragone, riscontro. Confrontare due cose per metterne in evidenza disparità e somiglianze.
(Fonte: Vocabolario della Lingua Italiana Zingarelli)

Utilizzo: atto, effetto dell'utilizzare. Rendere utile, mettere a profitto, sfruttare.
(Fonte: Vocabolario della Lingua Italiana Zingarelli)

Blocco: conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento. (Fonte: legge delega 127/2001 "Codice in materia del trattamento dei dati personali")

Interconnessione: atto, effetto dell'interconnettere. Collegamento fra diverse reti di comunicazione.
(Fonte: Vocabolario della Lingua Italiana Zingarelli)

Cancellazione: fare segni o fregi su ciò che è scritto o disegnato per renderlo illeggibile, annullarlo. Annullare, distruggere, eliminare, rimuovere da un programma, dalla coscienza, e simili.
(Fonte: Vocabolario della Lingua Italiana Zingarelli)

Distruzione: atto, effetto del distruggere. Ridurre al nulla, demolire completamente.
(Fonte: Vocabolario della Lingua Italiana Zingarelli)

Dato personale: qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

Dati identificativi: i dati personali che permettono l'identificazione diretta dell'interessato.

Dati sensibili: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Dati giudiziari: i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d. P. R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

Titolare: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Responsabile: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.

Incaricati: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

Interessato: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

Comunicazione: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Diffusione: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Dato anonimo: il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

Blocco: la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.

Banca di dati: qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

Garante: l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

Comunicazione elettronica: ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile.

Chiamata: la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale.

Reti di comunicazione elettronica: i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato.

Rete pubblica di comunicazioni: una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico.

Servizio di comunicazione elettronica: i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002.

Abbonato: qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate.

Utente: qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata.

Dati relativi al traffico: qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione.

Dati relativi all'ubicazione: ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico.

Servizio a valore aggiunto: il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione.

Posta elettronica: messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

Misure minime: il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto.

Strumenti elettronici: gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

Autenticazione informatica: l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.

Credenziali di autenticazione: i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.

Parola chiave: componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.

Profilo di autorizzazione: l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.

Sistema di autorizzazione: l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

3- Trattamento dei dati personali, elenco

Area tipologie e definizione di trattamento effettuate dal titolare

E' definita "trattamento" qualunque operazione, effettuata anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.

Le attività svolte dall'azienda nell'esercizio della sua attività sono indicate nel documento

- Allegato 2 "**TIPO TRATTAMENTO DATI PERSONALI**".

Notifica dei dati trattati

Ai sensi del Regolamento Europeo 2016/679 e delle successive interpretazioni del Garante per la protezione dei dati personali, non vi è l'obbligo di invio/comunicazione al Garante della notificazione del trattamento di dati personali effettuato.

4- Compiti – Doveri - Responsabilità - Incaricati - Archivi e Banche Dati

Il Titolare del trattamento

Definisce la Politica della Sicurezza dei dati personali

- stabilisce gli obiettivi che essa deve perseguire;
- identifica gli impegni e assegna le risorse necessarie al corretto funzionamento del Sistema Sicurezza, al fine di applicare e predisporre le misure di sicurezza idonee alla tutela dei dati trattati.

Obiettivi all'attuazione della tutela dei dati personali trattati

Impegni dell'Azienda:

. definire la finalità del trattamento dei dati

. definire le modalità del trattamento dei dati

. definire gli strumenti utilizzati per il trattamento dei dati

. definire i profili di sicurezza

Modus operandi:

. individuazione in forma scritta degli incaricati al trattamento dei dati

. predisposizione delle misure minime di sicurezza

. elaborazione del manuale annuale di DATA PROTECTION

. vigilanza sulla corretta osservanza degli obblighi di legge e dei diritti riconosciuti dalla legge agli interessati

. formazione del personale del personale relativamente alle disposizioni previste dal Codice Europeo in materia di protezione dei dati personali

Luoghi di trattamento dei dati: definizioni

Le definizioni dei luoghi di trattamento dei dati sono specificate nel documento

- Allegato 3 "**DEFINIZIONI DEI LUOGHI DI TRATTAMENTO DEI DATI**".

Elenco archivi cartacei ed informatici di conservazione dei dati

Le attività svolte dall'azienda nell'esercizio della sua attività sono specificate nel documento

- Allegato 4 "**ARCHIVI INFORMATICI E CARTACEI**".

Elenco Banche Dati – tipologia – categoria – luogo di conservazione

L'elenco con le informazioni delle banche dati sono specificate nel documento

- Allegato 5 "**BANCHE DATI**".

Compiti, responsabilità, organigramma ed incarichi

L'elenco dei responsabili è specificato nel documento

- Allegato 8 "**NOMINE RESPONSABILI ED INCARICATI**".

Chi sono e cosa devono fare:

Titolare del trattamento dei dati personali

Quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo, titolare del trattamento è l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza.

Responsabili del trattamento dei dati personali, compiti ed attribuzioni

Devono definire:

. la finalità del trattamento dei dati;

. le modalità del trattamento dei dati;

. gli strumenti utilizzati per il trattamento dei dati;

. i profili di sicurezza;

A tale scopo provvedono alla:

. individuazione in forma scritta degli incaricati al trattamento dei dati;
. predisposizione delle misure minime di sicurezza;
. elaborazione del **MANUALE DI DATA PROTECTION**;
. vigilanza sulla corretta osservanza degli obblighi di legge e dei diritti riconosciuti dalla legge agli interessati;
. formazione del personale relativamente alle disposizioni previste dal Codice Europeo in materia di protezione dei dati personali;
. se il trattamento è effettuato con mezzi informatici, redigere ed aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione;
. definire e successivamente verificare con cadenza semestrale le modalità di accesso ai locali e le misure da adottare per la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità come specificato in seguito;
. garantire che tutte le misure di sicurezza riguardanti i dati personali siano applicate;
. redigere ed aggiornare ad ogni variazione l'elenco delle sedi in cui vengono trattati i dati;
. redigere ed aggiornare ad ogni variazione l'elenco degli uffici in cui vengono trattati i dati;
. redigere ed aggiornare ad ogni variazione l'elenco delle banche dati oggetto di trattamento;
. decidere se affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare;
. qualora il trattamento dei dati sia stato affidato in tutto o in parte all'esterno della struttura del titolare controllare e garantire che tutte le misure di sicurezza riguardanti i dati personali siano applicate;
. se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più Responsabili della gestione e della manutenzione degli strumenti elettronici;

. se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più Incaricati della custodia delle copie delle credenziali qualora vi sia più di un incaricato del trattamento;
. se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più Incaricati delle copie di sicurezza delle banche dati;
. nominare gli incaricati del trattamento per le Banche di dati che gli sono state affidate;
. di sorvegliare che il trattamento sia effettuato nei termini e nei modi stabiliti dal Codice Europeo in materia di dati personali;
. di dare le istruzioni adeguate agli incaricati del trattamento effettuato con strumenti elettronici e non, periodicamente, e comunque almeno annualmente, verifica la sussistenza delle condizioni per la conservazione dei profili di autorizzazione degli incaricati del trattamento dei dati personali.

Amministratore di Sistema

Compiti ed attribuzioni:

. mantenere in efficienza il Sistema Informativo, sia per quanto concerne il software che l'hardware;
. comunicare al Titolare eventuali esigenze di installazione di nuovo software o hardware ed attenersi alle sue disposizioni;
. realizzare, in proprio e/o tramite personale delle aziende fornitrici e/o di consulenti eventualmente preposti, quanto richiesto dal Piano di adeguamento delle misure di sicurezza di cui al **MANUALE DI DATA PROTECTION**, limitatamente a ciò che concerne il Sistema Informativo;
. eseguire, in proprio e/o tramite personale delle aziende fornitrici, eventuali interventi sull'hardware e sul software, per nuove installazioni, normale manutenzione o anomalie; se il tempo richiesto per l'intervento, compreso quello per "Disaster Recovery", è superiore a 7 giorni, dovrà mettere a disposizione dell'utente una postazione, anche temporanea, che contenga gli stessi dati e fornisca le stesse prestazioni;
. relazionare al Titolare, su richiesta dello stesso, circa lo stato del Sistema Informativo, il livello di servizio fornito all'utenza e lo stato di avanzamento di eventuali interventi sull'hardware o sul software;
. controllare periodicamente che il software antivirus sia aggiornato;
. controllare periodicamente che il software del firewall sia aggiornato;
. se non è disponibile un sistema automatico di aggiornamento del software di sistema, aggiornare almeno ogni 30 giorni solari le patch del sistema operativo;
. e altre operazioni necessarie al fine di ridurre al minimo tutti gli eventuali rischi connessi alla gestione del Sistema Informativo.

Incaricati della custodia delle credenziali di autenticazione

Compiti:

. gestire e custodire le credenziali per l'accesso ai dati degli Incaricati del trattamento;
. predisporre, per ogni incaricato del trattamento, una busta sulla quale è indicato il nome dell'incaricato e all'interno della busta deve essere indicata la credenziale usata. Le buste con le credenziali debbono essere conservate in luogo chiuso e protetto;
. istruire gli incaricati del trattamento sull'uso delle parole chiave, sulle caratteristiche che debbono avere, e sulle modalità per la loro modifica in autonomia;
. revocare tutte le credenziali non utilizzate in caso di perdita della qualità che consentiva all'incaricato l'accesso ai dati personali;
. revocare le credenziali per l'accesso ai dati degli incaricati del trattamento nel caso di mancato utilizzo per oltre 6 mesi;
. adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Incaricati delle copie di sicurezza delle banche dati

Compiti:

. prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di sicurezza secondo i criteri stabiliti dal Responsabile della sicurezza dei dati personali; in particolare dovrà effettuare un back-up giornaliero;
. di provvedere a conservare con la massima cura e custodia i dispositivi utilizzati per le copie di sicurezza, impedendo l'accesso agli stessi dispositivi da parte di personale non autorizzato;
. assicurarsi della conservazione delle copie di sicurezza in luogo adatto e sicuro e ad accesso controllato;
. assicurarsi della qualità delle copie di sicurezza dei dati e della loro conservazione in luogo adatto e sicuro;
. di segnalare tempestivamente al Responsabile della gestione e della manutenzione degli strumenti elettronici, ogni eventuale problema dovesse verificarsi nella normale attività di copia delle banche dati.

In relazione agli incarichi affidati, gli incaricati dovranno:

. fornire al titolare o al responsabile, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire loro di svolgere efficacemente la propria attività di controllo;
. in generale, prestare la più ampia e completa collaborazione al titolare ed al responsabile al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente.

Incaricati manutenzione strumenti elettronici

Compiti:

. assicurarsi del corretto funzionamento degli strumenti elettronici;

. fornire al titolare o al responsabile, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire loro di svolgere efficacemente la propria attività di controllo;

. in generale, prestare la più ampia e completa collaborazione al titolare ed al responsabile al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente.

Incaricati del trattamento dati

Doveri:

. trattare i dati personali nella misura necessaria e sufficiente alle finalità proprie della banca dati nella quale vengono inseriti;

. adottare, nel trattamento dei dati, tutte le misure di sicurezza che siano indicate, oggi o in futuro, dal titolare o dal responsabile, in particolare dovrà:

a) per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su terminali altrui e/o di lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;

b) trattare i soli dati la cui conoscenza sia necessaria e sufficiente per lo svolgimento delle operazioni da effettuare;

c) conservare i supporti informatici e/o cartacei contenenti i dati personali in modo da evitare che detti documenti siano accessibili a persone non autorizzate al trattamento dei dati medesimi;

d) con specifico riferimento agli atti e documenti cartacei contenenti dati personali ed alle loro copie, restituire gli stessi al termine delle operazioni affidate o riporli nel loro luogo di conservazione;

e) utilizzare i supporti di memorizzazione usati solamente qualora i dati in essi precedentemente contenuti non siano in alcun modo recuperabili, altrimenti etichettarli e riporli negli appositi contenitori;

f) in caso si constati o si sospetti un incidente di sicurezza deve essere data immediata comunicazione al responsabile del trattamento;

- segnalare al titolare o al responsabile eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle predette misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;

- effettuare la comunicazione e la diffusione dei dati esclusivamente ai soggetti indicati dal titolare o dal responsabile e secondo le modalità stabilite dai medesimi;

- mantenere, salvo quanto precisato al punto precedente, 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;
- svolgere, in ogni caso, il trattamento dei dati personali per le finalità e secondo le modalità stabilite, anche in futuro, dal titolare e dal responsabile e, comunque, in modo lecito e secondo correttezza;
- fornire al titolare o al responsabile, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire loro di svolgere efficacemente la propria attività di controllo;
- in generale, prestare la più ampia e completa collaborazione al titolare ed al responsabile al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente.

5- Rischi sui dati personali - analisi e calcolo

Calcolo dei parametri da inserire nelle schede di valutazione

Attribuzione Valore (score in inglese) di pericolo (SP) ed azione correttiva

- Ad ogni punto di controllo presente in una check-list pericoli (CLP) è associato un valore (in inglese *score*) di pericolo (SP);
- quando un punto di controllo non è verificato (es. manca il Sistema di Backup dei dati), allora comparirà nella scheda di valutazione l'azione correttiva relativa (es. "Installare programma per il Backup e ripristino dati") ed il relativo score di pericolo (SP).

P: probabilità (corrispondenza al rischio – definizioni e criteri)

Consideriamo N. 04 livelli di probabilità

Specifiche dei Livelli ed eventuali conseguenze

Livello **P 1**: **Improbabile**

L'eventuale mancanza rilevata può provocare un danno per la concomitanza di più eventi poco probabili indipendenti. Sono estremamente rari episodi già verificatisi Il verificarsi del danno susciterebbe incredulità.

Livello **P2**: **Poco probabile**

La mancanza rilevata può provocare un danno solo in circostanze sfortunate di eventi. Sono noti, rari episodi già verificatisi. Il verificarsi del danno ipotizzato susciterebbe grande sorpresa.

Livello **P3**: **Probabile**

La mancanza rilevata può provocare un danno, anche se non in modo automatico o diretto. E' noto qualche episodio in cui alla mancanza ha fatto seguito il danno. Il verificarsi del danno ipotizzato, susciterebbe una moderata sorpresa in azienda.

Livello **P4**: **Altamente probabile**

Esiste una correlazione diretta tra la mancanza rilevata ed il verificarsi del danno ipotizzato. Si sono già verificati danni per la stessa mancanza rilevata nella stessa Azienda o in azienda simile o in situazioni operative simili.

R: rischio (Calcolo del rischio R e tempi di intervento)

Per ogni punto di una CLP non verificato (associato al relativo score di pericolo SP) occorre calcolare il rischio legato a quella mancanza (es. mancanza del sistema di Backup).

Il rischio R è dato dallo score di pericolo SP moltiplicato per la probabilità P.

R= SP x P

A seconda dei valori di P e SP ottengo sulla base della matrice sotto riportata una classificazione del rischio in tre fasce, contraddistinte da un colore.

La valutazione delle azioni correttive è determinata dalla Zona (colore)

. **ZONA VERDE**: situazione **MIGLIORABILE**

il rischio è tale da richiedere un'**eventuale azione DA PROGRAMMARE**

. ZONA GIALLA: situazione **CARENTE**

il rischio è tale da richiedere un'**azione correttiva in tempo x**

. ZONA ROSSA: situzione **MOLTO CARENTE**

il rischio è tale da richiedere un'**azione correttiva IMMEDIATA**

All'interno di una stessa zona (esempio zona rossa) si elencano per prime le azioni correttive con valore di R più elevato.

SCHEMA/INDICAZIONE DELLA TEMPISTICA DI ESECUZIONE DELLE AZIONI CORRETTIVE E LORO VALUTAZIONE

Tipo zona	Valutazione	Tempi di esecuzione	
VERDE	MIGLIORABILE	Se R = 1	Rispecchia misure minime di sicurezza
		Se R = 2	Da programmare
GIALLA	CARENTE	Se 2>R<=4	Massimo 6 mesi
		Se 2>R<=6	Massimo 3 mesi
ROSSA	MOLTO CARENTE	Se R>6	Immediato

Comprensione dei rischi sui dati personali

L'elenco con le informazioni sui rischi e specificato nel documento:

- Allegato 9 "**ESEMPI DI RISCHIO**"

6- Misure di sicurezza

Indicazioni necessarie delle misure in essere e da adottare a contrasto dei rischi individuati dall'analisi dei rischi.

Per misura si intende:

. lo specifico intervento tecnico od organizzativo posto in essere per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia;
. tutte quelle attività di verifica e controllo nel tempo, essenziali per assicurarne l'efficacia. Senza procedure di controllo periodico, infatti, nessuna misura può essere considerata completa.

Le misure da adottare per garantire l'integrità e la disponibilità dei dati sono indicate dal **Manuale di Data Protection**, corredato di allegati che inoltre indicano i provvedimenti che il titolare, il responsabile (ove designato) e l'incaricato devono mettere in atto per garantire il livello minimo di sicurezza dei dati in loro possesso.

1- E' necessario un sistema di autenticazione degli incaricati e dei responsabili che hanno accesso ai dati. Questo sistema di autenticazione serve a garantire un accesso ai dati limitato agli operatori incaricati del trattamento degli stessi.

   a) Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato ad una parola chiave riservata conosciuta solamente dal medesimo (ID e PASSWORD) oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato (Smart Card), oppure in una caratteristica biometria dell'incaricato (scansione della retina), eventualmente associati ad un codice identificativo o ad una parola chiave.

   b) Ad ogni incaricato si possono assegnare una o più credenziali per l'autenticazione.

   c) Se il sistema di autenticazione richiede una parola chiave, quest'ultima deve essere composta da almeno otto caratteri (possibilmente alfanumerici) oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito. La parola chiave non deve contenere riferimenti agevolmente riconducibili all'incaricato ed essere modificata da quest'ultimo al primo utilizzo. La parola chiave deve essere cambiata almeno ogni sei mesi e nel caso di trattamento di dati sensibili o giudiziari ogni tre. Il codice di identificazione, dove utilizzato non può essere assegnato ad altri incaricati neppure in tempi diversi.

   d) Le credenziali di autenticazione se non utilizzate da almeno sei mesi devono essere disattivate (ad esclusione di quelle preventivamente autorizzate per scopi di gestione tecnica); lo stesso provvedimento vale per le credenziali degli incaricati che perdono la qualità che consente loro di accedere ai dati.

   e) Quando l'accesso ai dati è consentito esclusivamente mediante uso della credenziale di autenticazione, sono impartite preventive disposizioni scritte volte a garantire la disponibilità dei dati in caso di prolungata assenza da parte dell'incaricato e si renda indispensabile intervenire per necessità di operatività e di sicurezza. In questo caso la custodia delle copie delle credenziali è destinata a soggetti preventivamente incaricati.

   f) Periodicamente, almeno annualmente, deve essere verificata la sussistenza delle condizioni per la conservazione delle credenziali di autenticazione e conseguentemente stilata una lista degli incaricati che può essere redatta per classi omogenee di incarico.

2- I dati devono essere protetti contro il rischio di intrusione e dell'azione di programmi mediante l'attivazione di idonei strumenti (Firewall e Antivirus) da aggiornare con cadenza almeno semestrale; inoltre devono essere aggiornati i programmi volti a prevenire la vulnerabilità dei sistemi elettronici (Antivirus) e a correggerne difetti (patch); questi aggiornamenti devono essere effettuati almeno con cadenza annuale e nel caso si tratti di dati sensibili o giudiziari l'aggiornamento è semestrale (sarebbe opportuno un aggiornamento almeno settimanale);

3- Deve essere impostato un sistema di salvataggio dei dati volto al recupero di possibili perdite dati, con cadenza almeno settimanale (Sistema di backup). Il sistema di ripristino dei dati deve garantire l'accesso agli stessi entro tempi compatibili con i diritti degli interessati e comunque non superiore ai sette giorni;

4- L'utilizzo e la custodia di supporti rimovibili per il trasferimento o l'elaborazione dei dati va disciplinato al fine di evitare trattamenti non consentiti. I supporti rimovibili contenenti dati sensibili o giudiziari non utilizzati vanno distrutti o resi inutilizzabili. Gli organismi sanitari devono trattare i dati sensibili contenuti in elenchi, registri o banche di dati tenuti con l'ausilio di strumenti elettronici utilizzando tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni al fine di consentire il trattamento disgiunto dei medesimi dagli altri dati personali;

5- Il titolare che adotta misure minime di sicurezza avvalendosi della collaborazione di soggetti esterni alla propria struttura deve richiedere da questi una descrizione scritta dell'intervento effettuato che ne attesta la conformità;

6- I dati relativi all'identità genetica devono essere trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi. Il trasporto dei dati genetici all'esterno deve avvenire in contenitori muniti di serratura o tramite dispositivi equipollenti. Il trasferimento dei dati in formato elettronico deve avvenire mediante apposite tecniche di cifratura;

7- Gli atti ed i documenti cartacei contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti devono essere controllati e custoditi dagli incaricati stessi fino alla restituzione per evitare che ad essi possano accedere persone prive di autorizzazione.

Misure di sicurezza in essere e da adottare

Le misure di sicurezza in essere e le misure di sicurezza da adottare sono specificate nel documento:

- Allegato 10 "**PROGRAMMA DI INTERVENTO**"

7- Dati digitali: disponibilità, criteri e modalità di ripristino

Descrizione dei criteri e delle procedure adottate per il salvataggio dei dati e per il loro ripristino in caso di danneggiamento o di inaffidabilità della base dati.

L'importanza di queste attività deriva direttamente dalla eccezionalità delle situazioni in cui il ripristino ha luogo: è essenziale che, quando necessarie, le copie dei dati siano disponibili e le procedure efficaci.

A seguire le tabelle riassuntive dei processi di Backup (Tabelle Backup) e ripristino dei dati (Tabelle Ripristino).

Tabelle di Backup e Tabelle di Ripristino sono specificate nel documento:

- Allegato 4 "**ARCHIVI INFORMATICI E CARTACEI**"

8- Cifratura dei dati o separazione dei dati identificativi

Sezione riservata agli **organismi sanitari e agli esercenti professioni sanitarie.**

Modalità di protezione adottate in relazione ai dati per cui è richiesta la cifratura – o la separazione fra dati identificativi e dati sensibili – nonché le modalità con cui viene assicurata la sicurezza di tali trattamenti.

Le tabelle di ripristino riassuntive relative al trattamento dei dati effettuati (se applicabili), alla relativa protezione scelta e alle modalità utilizzate sono specificate nel documento:

- Allegato 6 "**DATI SANITARI**"

9- PIANIFICAZIONE DELLA FORMAZIONE

Il titolare del trattamento deve provvedere a formare i responsabili e gli incaricati che si occupano effettivamente della gestione dei dati.

Il **MANUALE DI DATA PROTECTION** contiene, con i suoi allegati, "la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali".

Piano di formazione - La previsione di interventi di formazione è stata prevista in diversi momenti della vita lavorativa. E' indispensabile provvedere sia ad una formazione all'atto della nomina, sia ad una formazione continua, orientativamente una volta all'anno e comunque ogni qualvolta ci siano dei cambiamenti rilevanti nella gestione dei rischi, delle misure minime di sicurezza e delle modalità di ripristino dei dati.

Il piano di formazione è specificato nel documento denominato:

- Allegato 7 "**PIANO DI FORMAZIONE**"

L'evoluzione della formazione può essere redatta nel documento denominato:

- Allegato 11 "**REGISTRO DELLA FORMAZIONE**"

10- Dati trattati o comunicati in esterno

Ci sono casi in cui l'azienda, nell'organizzazione delle sue funzioni, delega alcune delle attività a terzi. In questi casi, i dati vengono quindi trattati, o semplicemente comunicati, al di fuori dell'azienda.

Obiettivo di questa sezione è redigere un quadro sintetico delle banche dati trasferite o gestite da terzi che comportano il trattamento di dati personali, con l'indicazione del responsabile del trattamento in riferimento alla protezione dei dati personali.

E' indispensabile che il soggetto che tratta i dati in out-sourcing (ossia l'ente o professionista esterno) garantisca su base contrattuale di rispettare quanto previsto dal Regolamento Europeo 2016/679. In particolare il soggetto cui le attività sono affidate deve dichiarare:

1. di essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali, sono soggetti all'applicazione del codice per la protezione dei dati personali;
2. di ottemperare agli obblighi previsti dal Regolamento Europeo per la protezione dei dati personali;
3. di adottare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o di integrarle nelle procedure già in essere;
4. di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate e di allertare immediatamente il proprio committente in caso di situazioni anomale o di emergenze;
5. di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

Il trattamenti affidati all'esterno sono specificati nel documento denominato:

- Allegato 12 "**TRATTAMENTO DEI DATI AFFIDATI ALL'ESTERNO**".

11- Approvazione del MANUALE DI DATA PROTECTION

MANUALE
DI DATA PROTECTION

AL FINE DI OTTEMPERARE ALLE DISPOSIZIONI DEL REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO DEL 27 APRILE 2016

_____lì, _____

Il Titolare del trattamento

_____