Revisione
00
Anno
2020

REGOLAMENTO EUROPEO 2016/679

Manuale Privacy

BETA RICAMBI DI MARTINETTO ROBERTO SERGIO

Sommario

Capitolo

1

Introduzione

Generalità

Il Regolamento Europeo 2016/679, entrato in vigore il 25 Maggio 2016 e applicativo dal 25 Maggio 2018, disciplina la normativa in materia di tutela della privacy, partendo dal presupposto che “Chiunque ha diritto alla protezione dei dati personali che lo riguardano”.

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, il ripristino della disponibilità dei dati e dei sistemi;
g) tenuta di un aggiornato manuale della privacy;
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 presente Manuale Privacy è redatto per definire tutte le misure minime di sicurezza che ha adottato e che debbono essere adottate in via preventiva dall’azienda, conformemente a quanto previsto dal Regolamento Europeo Privacy UE/2016/679.

Nel Manuale Privacy 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.

Campo di applicazione

Il Manuale Privacy definisce le politiche e gli standards 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.

Il presente Documento Programmatico sulla Sicurezza riguarda il trattamento di tutti i dati personali:

. Personali
. Identificativi
. Sensibili
. Genetici
. Biometrici

trattati con:

. Strumenti elettronici di elaborazione
. Altri strumenti di elaborazione

Il Documento deve essere conosciuto ed applicato da tutte le funzioni che fanno parte dell'organizzazione.

Informazioni minime del Manuale Privacy

Il Regolamento prevede che il Manuale Privacy sia definito con un contenuto informativo minimo, cioè è indispensabile che contenga:

l’elenco dei trattamenti di dati personali;

la distribuzione dei compiti e delle responsabilità nell’ambito delle strutture preposte al trattamento dei dati;

l’analisi dei rischi che incombono sui dati;

le 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;

la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;

la previsione di interventi formativi 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;

la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in
caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;

per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Finalità

Le misure individuate perseguono la finalità 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 presente documento 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 presente documento 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 presente documento è aderente alle 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.

Capitolo
2

Anagrafica aziendale

Dati Identificativi

Ditta rag. soc. BETA RICAMBI DI MARTINETTO ROBERTO SERGIO

Sede legale	TORINO (TO) CORSO GROSSETO 247/B
Sede operativa per il Manuale Privacy	TORINO (TO) CORSO GROSSETO 247/B
mail	amministrazione@betaricambi.com

Distribuzione dei compiti e delle responsabilità

Titolare del trattamento dei dati personali	MARTINETTO ROBERTO SERGIO
Responsabili del trattamento dei dati personali	MARTINETTO ROBERTO SERGIO
Incaricati del trattamento dei dati personali	MARTINETTO ROBERTO SERGIO
Incaricati della gestione e della manutenzione degli strumenti elettronici	MARTINETTO ROBERTO SERGIO
Incaricati delle copie di sicurezza delle banche dati	MARTINETTO ROBERTO SERGIO
Incaricati della custodia delle copie delle credenziali	MARTINETTO ROBERTO SERGIO
Responsabili uffici	MARTINETTO ROBERTO SERGIO

Descrizione dell'attività svolta

Codice: 45.32 - commercio al dettaglio di parti e accessori di autoveicoli

Capitolo

3

Riferimenti normativi

1. REGOLAMENTO EUROPEO 2016/679

Definizioni

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 od 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.

Capitolo

4

Elenco del trattamento dei dati personali

Trattamento di dati personali

In questa sezione sono riportate le tipologie di trattamento effettuate dal titolare.

Si definisce “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.

Si specifica che le attività svolte dall’azienda nell’esercizio della sua attività sono specificate nel documento allegato denominato “Dichiarazione di metodologia allegato 2”.

Notifica dei dati trattati

Ai sensi del Regolamento Europeo 2016/679 e delle successive interpretazioni del Garante per la protezione dei dati personali, l'Organizzazione non è tenuta ad inviare al Garante stesso la notificazione del trattamento di dati personali effettuato.

Capitolo
5

Organigramma dei compiti e delle responsabilità

Responsabilità

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

Per l'attuazione della tutela dei dati personali trattati, l'Azienda si impegna a porre in essere quanto di seguito espresso:
. 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

a tale scopo provvede alla:

. individuazione in forma scritta degli incaricati al trattamento dei dati
. predisposizione delle misure minime di sicurezza
. elaborazione del manuale annuale della privacy
. 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

Definizione dei luoghi di trattamento dei dati

Le definizioni dei luoghi di trattamento dei dati sono specificate nel documento allegato denominato ***"Dichiarazione di metodologia allegato 3***".

Elenco archivi cartacei di conservazione dei dati

Le attività svolte dall'azienda nell'esercizio della sua attività sono specificate nel documento allegato denominato ***"Dichiarazione di metodologia allegato 4"***.

Elenco archivi informatici di conservazione dei dati

L'elenco archivi informatici di conservazione dei dati è specificato nel documento allegato denominato ***"Dichiarazione di metodologia allegato 4"***.

Organigramma dei compiti e delle responsabilità

L'elenco dei responsabili è specificato nel documento allegato denominato ***"Dichiarazione di metodologia allegato 8"***.

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:
. 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;

a tale scopo provvedono alla:

- individuazione in forma scritta degli incaricati al trattamento dei dati;
- predisposizione delle misure minime di sicurezza;
- elaborazione del manuale privacy;
- 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 acceso 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 Privacy, 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 metter 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.

Gli incaricati della custodia delle credenziali di autenticazione hanno il compito di:

- 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

Gli incaricato delle copie di sicurezza delle banche dati hanno il compito di:

- . 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

Gli incaricati della manutenzione degli strumenti elettronici hanno il compito di:

- 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.

In particolare dovranno:
- 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.

Capitolo
6

Analisi dei rischi

Calcolo dei parametri da inserire nelle schede di valutazione

Attribuzione Score di pericolo (SP) ed azione correttiva
Ad ogni punto di controllo presente in una check-list pericoli (CLP) è associato uno 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).

Calcolo della probabilità P

Probabilità P	Livello	Definizioni / criteri
4	Altamente probabile	Esiste una correlazione diretta tra la mancanza rilevata ed il verificarsi del danno ipotizzato per i lavoratori Si sono già verificati danni per la stessa mancanza rilevata nella stessa Azienda o in azienda simile o in situazioni operative simili Il verificarsi del danno conseguente la mancanza rilevata non susciterebbe alcuno stupore in azienda
3	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
2	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
1	Improbabile	La 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

Calcolo del rischio R e dei 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.

. ZONA ROSSA: il rischio è tale da richiedere un'azione correttiva MOLTO CARENTE
. ZONA GIALLA: il rischio è tale da richiedere un'azione correttiva CARENTE
. ZONA VERDE il rischio è tale da richiedere un'azione correttiva MIGLIORABILE

La valutazione delle azioni correttive è determinata dalla Zona (colore).
All'interno di una stessa zona (esempio zona rossa) si elencano per prime le azioni correttive con valore di R più elevato.

Indicazione della tempistica di esecuzione delle azioni correttive e loro valutazione

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

Capitolo

7

Misure in essere e da adottare

In questa sezione sono riportate, in forma sintetica, le 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 sancite dal presente manuale privacy corredato di allegati che inoltre indica 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

Le misure di sicurezza in essere è specificato nel documento allegato denominato ***"Dichiarazione di metodologia allegato 10":***

Misure di sicurezza da adottare

Le misure di sicurezza da adottare è specificato nel documento allegato denominato ***"Dichiarazione di metodologia allegato 10":***

Capitolo

8

Criteri e modalità di ripristino della disponibilità dei dati

Contenuti

In questa sezione sono descritti i criteri e le procedure adottati 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, quando sono necessarie, le copie dei dati siano disponibili e le procedure efficaci.
Qui di seguito le tabelle riassuntive dei processi di Backup (Tabelle Backup) e ripristino dei dati (Tabelle Ripristino).

Tabelle Backup

Le tabelle di back-up sono specificate nel documento allegato denominato ***"Dichiarazione di metodologia allegato 4":***

Tabelle Ripristino

Le tabelle di ripristino sono specificate nel documento allegato denominato ***"Dichiarazione di metodologia allegato 4":***

Capitolo
9

Cifratura dei dati o separazione dei dati identificativi

Contenuti

In questa sezione, riservata agli organismi sanitari ed agli esercenti professioni sanitarie, sono rappresentate le modalità di protezione adottate in relazione ai dati per cui è richiesta la cifratura – o la separazione fra dati identificativi e dati sensibili – nonché 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 denominato ***"Dichiarazione di metodologia allegato 6":***

Capitolo
10

Pianificazione degli interventi formativi previsti

Premessa

Per un corretto trattamento dei dati è opportuno che il titolare del trattamento provveda a formare i responsabili e gli incaricati che si occupano effettivamente della gestione dei dati.

Il Regolamento Europeo richiede infatti che il Manuale Privacy contenga "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 allegato denominato ***"Dichiarazione di metodologia allegato 7".***

Capitolo
11

Trattamenti affidati all'esterno

Premessa

L'azienda, nell'organizzazione delle sue funzioni, delega alcune delle attività a terzi.
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 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.

II trattamenti affidati all'esterno sono specificati nel documento allegato denominato ***"Dichiarazione di metodologia allegato 12".***

Capitolo
12

Approvazione manuale privacy

_____lì,_____

Il Titolare del trattamento

_____

ALLEGATO 1

DATI DELL'AZIENDA

Società	BETA RICAMBI DI MARTINETTO ROBERTO SERGIO
Unità operativa	TORINO
Indirizzo	CORSO GROSSETO 247/B

Descrizione dell'attività svolta (connessa al trattamento dei dati)

COMMERCIO AL DETTAGLIO DI PARTI E ACCESSORI DI AUTOVEICOLI.

ALLEGATO 2

TIPO TRATTAMENTO DATI PERSONALI DEL CLIENTE

Tipo Trattamento dati personali dei clienti

Raccolta	x	Registrazione	X	Organizzazione	x	Conservazione	X	Consultazione	x
Elaborazione	X	Modificazione	//	Selezione	X	Estrazione	//	Raffronto	//
Utilizzo	X	Interconnessione	X	Blocco	//	Cancellazione	X	Diffusione	//
Distruzione	//	Comunicazione	x						

Finalità del trattamento: NON E' PRESENTE NESSUNA FINALITA'. ALTRO:

Entriamo in possesso dei dati dei clienti tramite

Elenchi pubblici	//	Visure camerali	//	Albi	//
Associazioni di categoria	//	Attività di marketing	//	Comunicati dai clienti	X
Altro	//				

Di quali dati comuni dei clienti siete in possesso?

Anagrafica	X	Dati bancari	X	Bilanci	//
Consulenti	//	Collaboratori	//	Dati da visure camerali	//
Elenco dipendenti	//	Altri	//	//	

Come conservate i dati identificativi dei clienti?

Materiale cartaceo	//	Elaboratore elettronico	//	Cartaceo ed elettronico	x

Comunicate i dati dei clienti all'estero	//	Comunicate i dati dei clienti all'esterno	x

Se comunicate i dati all'esterno, a chi vengono comunicati?

Fornitori	//	Clienti	//	Banche	X
Altro	//				

Siete in possesso di dati sensibili	//
Di quali dati sensibili dei vostri clienti siete in possesso? ////	

DICHIARAZIONE DI METODOLOGIA

ALLEGATO 2

[redacted]

Tipo Trattamento dati personali dei fornitori

Raccolta	X	Registrazione	X	Organizzazione	X	Conservazione	X	Consultazione	X
Elaborazione	X	Modificazione	//	Selezione	X	Estrazione	//	Raffronto	//
Utilizzo	X	Interconnessione	X	Blocco	//	Cancellazione	X	Diffusione	//
Distruzione	//	Comunicazione	x						

Finalità del trattamento: I dati personali dei fornitori vengono trattati allo scopo di adempiere agli obblighi derivanti dal contratto, per assolvere agli obblighi civilistici e fiscali, nonché per la tenuta della contabilità.

Entriamo in possesso dei dati dei fornitori tramite

Elenchi pubblici	//	Visure camerali	//	Albi	//
Associazioni di categoria	//	Attività di marketing	x	Comunicati dai clienti	//

Siamo in possesso dei seguenti dati dei nostri fornitori

Per comunicazione	X	Dati fiscali	X	Economici patrimoniali	//
Consulenti	//	Anagrafica	X	Bilanci	//
Visure camerali	//	Dati bancari	X	Collaboratori	//

Conserviamo i dati identificativi dei Fornitori

Materiale cartaceo	//	Elaboratore elettronico	//	Cartaceo ed elettronico	x

Se comunicate i dati all'esterno, a chi vengono comunicati?

Fornitori	//	Clienti	//	Banche	X
Altro	//	//			

Comunicate i dati dei fornitori all'esterno	x

Siete in possesso di dati sensibili	//

Di quali dati sensibili dei vostri fornitori siete in possesso? ////

ALLEGATO 2

Tipo Trattamento dati personali dei dipendenti

Raccolta	X	Registrazione	X	Organizzazione	X	Conservazione	X	Consultazione	X
Elaborazione	X	Modificazione	//	Selezione	//	Estrazione	//	Raffronto	//
Utilizzo	X	Interconnessione	//	Blocco	//	Cancellazione	X	Diffusione	//
Distruzione	//	Comunicazione	x						

Finalità del trattamento: I dati personali del personale dipendente vengono trattati ai fini dell'instaurazione, gestione ed estinzione del rapporto di lavoro, nonché dell'applicazione della normativa in materia di previdenza ed assistenza anche integrativa, o in materia di igiene e sicurezza del lavoro, nonché in materia fiscale, sindacale, di tutela della salute e per motivi di tenuta della contabilità e di corresponsione di stipendi, emolumenti e/o benefici accessori

Entriamo in possesso dei dati dei dipendenti tramite

Agenzie internali	//	Aziende specializzate	//	Curriculum ricevuti	x

Come conservate i dati identificativi dei Dipendenti?

Materiale cartaceo	//	Elaboratore elettronico	//	Cartaceo ed elettronico	x

Comunicate i dati dei clienti all'esterno	x

Siamo in possesso dei seguenti dati dei dipendenti

Per comunicazione	X	Dati fiscali	X	Derivanti da busta paga	X
Dati contrattuali	x				

Conserviamo i dati identificativi dei dipendenti	//

ALLEGATO 2

[redacted]

Tipo Trattamento dati personali dei altri soggetti

Raccolta	//	Registrazione	X	Organizzazione	//	Conservazione	X	Consultazione	x
Elaborazione	//	Modificazione	//	Selezione	//	Estrazione	//	Raffronto	//
Utilizzo	X	Interconnessione	//	Blocco	//	Cancellazione	X	Diffusione	//
Distruzione		Comunicazione		Finalità del trattamento: Avvocato. Commercialista. Direttore di banca. Notaio. Banca. Consulenza sicurezza sul lavoro. Consulente del lavoro. Prestatori di opera di vario tipo. Altro:					

Definizione dei luoghi di trattamento dei dati

Area di pertinenza	UFFICIO	Responsabile dell'area di pertinnza	MARTINETTO ROBERTO SERGIO
Area di pertinenza	///	Responsabile dell'area di pertinnza	///////////////////////////////////////

Conserviamo i dati identificativi dei altri soggetti

Materiale cartaceo	//	Elaboratore elettronico	//	Cartaceo ed elettronico	x

Siete in possesso di dati sensibili	//	//
	Di quali dati sensibili siete in possesso?	

Si intende per altri soggetti

AVVOCATO. COMMERCIALISTA. DIRETTORE DI BANCA. NOTAIO. CONSULENZA SICUREZZA SUL LAVORO. CONSULENTE DEL LAVORO. PRESTATORI DI OPERA DI VARIO TIPO.

Finalità del trattamento: I dati personali degli altri soggetti vengono trattati allo scopo di adempiere agli obblighi derivanti dal contratto, per assolvere agli obblighi civilistici e fiscali .

Definizione dei luoghi di trattamento dei dati

Area di pertinenza	UFFICIO
Responsabile dell'area di pertinenza	MARTINETTO ROBERTO SERGIO

Area di pertinenza	//
Responsabile dell'area di pertinenza	//

ALLEGATO 3

DEFINIZIONE DEI LUOGHI DI TRATTAMENTO DEI DATI

Definizione dei luoghi di trattamento dei dati	
Area di pertinenza	**UFFICIO**
Responsabile dell'area di pertinenza	**MARTINETTO ROBERTO SERGIO**

Area di pertinenza	//////////
Responsabile dell'area di pertinenza	//////////

ALLEGATO 4

ARCHIVI INFORMATICI

Archivi informatici

Tipologia	Computer sand-alone	X	Computer in rete	X	Server	x

Tipo di supporto	Magnetico	//	Ottico	//	Solido	x

Sistema di protezione	Password	X	Firewall	X	Antivirus	x

Sistema di sicurezza	buckup	X	Periodicità	settimanale	Supporto	⌊COMPUTER
	N° di copie	⌊2⌋ oppure:	Luogo di conservazione delle copie		nas	
	Caratteristiche del luogo di conservazione del backup			⌊GENERICO⌋		
	Vengono effettuate prove di ripristino	//	Periodicità	//		
	Tempo stimato per il ripristino	//	Descrizione del ripristino dei dati	nas		

Sicurezza dei locali	Accesso vietato al pubblico	//	Sistema di allarme	x	Finestre con inferiate	x
	Estintori	X	Chiusura locale serratura	//	Sistema antincendio	//
	Videosorveglianza	x	NOTE:			

ALLEGATO 4

ARCHIVI CARTACEI

UFFICIO	X

Tipologia						
Armadio ignifugo con serratura	//	Archivio generico con serratura	X	Altro armadio senza serratura	//	
Classificatore/cassetto con serratura	//	Classificatore/cassetto senza serratura	//	Cassaforte	//	
Scaffalatura	//					

Sicurezza del locale					
Accesso non consentito al pubblico	X	Sistema di allarme	X	Finestre con inferiate	X
Chiusura locale on serratura	//	Sistema antincendio	//	Sistema di videosorveglianza	X
Estintori	x	NOTE			

ALLEGATO 5

BANCHE DATI

Nome Archivio	UFFICIO	Descrizione	⌊CARTACEO ED INFORMATICO⌋

Tipologia dei dati

Comuni	⌊SI⌋	Sensibili	⌊NO⌋	Giudiziari	⌊NO⌋

Categoria

Clienti	⌊SI⌋	Fornitori	⌊SI⌋	Dipendenti	⌊NO⌋	Altri soggetti	⌊NO⌋

Luogo conservazione

Ufficio	⌊SI⌋	Archivio informatico	NAS	Archivio cartaceo	⌊UFFICIO⌋

Come conservate i dati identificativi dei CLIENTI -DIPENDENTI -FORNITORI -ALTRI SOGGETTI ?

Materiale cartaceo	////////////////////////////////	Elaboratore elettronico	////////////////////////////////	Cartaceo ed elettronico	⌊SI⌋

Comunicate i dati all’estero	⌊NO⌋	Comunicate i dati all’esterno	⌊NO⌋

Se comunicate i dati all’esterno, a chi vengono comunicati?

Fornitori	//////////////////////	Clienti	//////////////////////	Banche	/////////////////////
Altro	//////////////////////	Siete in possesso di dati sensibili	//		

Responsabile e Luogo di conservazione		
MARTINETTO ROBERTO SERGIO	X	UFFICI

ALLEGATO 5

PC	X	ARCHIVI INFORMATICI

Sicurezza Informatica – Parte 1

I responsabili della manutenzione, se esterni alla ditta, hanno accesso alle banche dati?	⌊NO⌋
Con quali restrizioni?	

E' presente un sistema di autenticazione su tutte le macchine	⌊NO⌋

Dove sono conservate le credenziali di autenticazione?	

Le password hanno un numero di caratteri alfanumerici pari o superiore a 8?	⌊SI⌋

Contengono dati che possono ricondurre all'utente o alla ditta?	⌊SI⌋

Le password sono aggiornate periodicamente	⌊SI⌋	Ogni quanto?	⌊OGNI 6 MESI⌋

E' presente un sistema di sospensione dell'apparecchio elettronico in caso di mancato utilizzo temporaneo	⌊NO⌋

Al termine di tale sospensione è richiesta una password?	⌊NO⌋	Uguale a quella di accesso	//////////////////

E' prevista la distruzione o la rimozione di autenticazioni se non utilizzate per lunghi periodi?	⌊NO⌋

Ogni incaricato ha una sola autorizzazione consentita?	⌊SI⌋

L'autenticazione è data in base all'operatore o in base al supporto?	⌊SUPPORTO⌋

Esistono autenticazioni speciali?	⌊NO⌋

Se si, quali?	

Sicurezza Informatica – Parte 2

Che sistemi sono adotti per la protezione dei dati?	FIREWAL

E' installato un gruppo di continuità su tutte le macchine?	⌊SI⌋

I dati personali e i dati sensibili sono conservati sullo stesso database?	//////////////////////////

I dati sensibili vengono a terzi?	//////////////////////////

E' installato un programma antivirus su tutte le macchine?	SI	E' aggiornato periodicamente?	SI	Ogni quanto?	GIORNALMENTE

Sicurezza Informatica – Parte 3

E’ presente una connessione internet?	SI	Che tipo di connessione è?	⌊FIBRA⌋
E’ presente un firewall?	SI	E’ aggiornato periodicamente?	SI
Ogni quanto?	GIORNALMENTE	E’ stato testato	NO
Chi ha effettuato il test?		//	

Viene eseguito un controllo dei supporti informatici provenienti da altri enti o società? **⌊SI⌋ :** -ALL 12- nominativo: ///	⌊NO⌋

Sono state adottate cautele per garantire la segretezza della componente riservata delle credenziali (es. password), al fine di evitare il rischio della sottrazione delle credenziali da parte del personale incaricato?	⌊SI⌋

Il personale incaricato è stato adeguatamente formato sulla disciplina della tutela dei dati personali della tutela dei dati personali, sui rischi connessi al trattamento dei dati personali e sulle misure da adottare per evitare la perdita accidentali dei dati personali?	⌊SI⌋

In passato si sono verificati errori del personale incaricato che ha causato la perdita dei dati personali o l’accesso ai dati da parte di persone non autorizzate?	⌊NO⌋

DICHIARAZIONE DI METODOLOGIA

ALLEGATO 7

FORMAZIONE

PIANO DI FORMAZIONE

TIPOLOGIA DI FORMAZIONE	CLASSI DI INCARICO INTERESSANTE	PERIODICITA' DELLA FORMAZIONE	DURATA DELLA FORMAZIONE
Trattamento dati: rischi legati alla tipologia di dati trattati (sensibili)	Tutti gli incaricati generaci	Nel caso di cambio mansione o modifiche al Regolamento in vigore	2 ore
Trattamento dati: rischi legati alla tipologia di dati trattati (personali)	Tutto il personale coinvolto	Al momento dell’incarico	4 ore

ALLEGATO 8

NOMINA DI INCARICATO DEL TRATTAMENTO DI DATI PERSONALI

Il sottoscritto MARTINETTO ROBERTO SERGIO
in qualità di legale rappresentante della ditta BETA RICAMBI DI MARTINETTO ROBERTO SERGIO
con sede a TORINO
in C.SO GROSSETO 247/B CAP 10121

PREMESSO CHE

il Regolamento Europeo 2016/679, concernente la tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali fissa le modalità da adottare per detto trattamento ed individua i soggetti che, in relazione all'attività svolta, sono tenuti agli adempimenti previsti dallo stesso regolamento; - il suddetto regolamento prevede che "Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite. La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima" ;
- si intende procedere alla nomina degli incaricati dei trattamenti dei dati custoditi e gestiti da
MARTINETTO ROBERTO SERGIO

TUTTO CIO' PREMESSO
NOMINA

incaricato del trattamento dei dati personali il Sig/Sig.ra
MARTINETTO ROBERTO SERGIO
nello svolgimento di tale compito l' incaricato potrà accedere alle seguenti banche dati:

L'incaricato dovrà effettuare il trattamento dei dati nel rispetto della normativa vigente e delle misure di sicurezza indicate dal citato Regolamento Europeo 2016/679
L'incaricato dovrà, inoltre, rispettare le istruzioni impartite dal titolare o dal responsabile sia con il presente atto di nomina sia in seguito.
In particolare dovrà:

- fornire, al primo contatto con gli utenti, l' informativa e, se previsto, farsi rilasciare il relativo consenso;
- raccogliere i dati personali e registrarli unicamente per finalità inerenti l' attività svolta;
- verificare l' esattezza, la completezza e la pertinenza dei dati trattati;
- accedere ai dati limitatamente per l' espletamento delle proprie mansioni ed esclusivamente durante l' orario di lavoro, salvo espressa richiesta da parte del Titolare;
- sostituire, secondo le modalità previste nel seguito, le parole chiave (Password);
- verificare che i dati trattati, anche in caso di interruzione temporanea del lavoro, non siano accessibili a terzi non autorizzati, attivando lo screen saver e riponendo i supporti cartacei nella cassettiera della scrivania;
- avvisare l' Incaricato all' Amministrazione del Sistema in caso di anomalie del software, dell' hardware e, se si utilizza Internet o un sistema di posta elettronica, della presunta presenza di virus informatici;
- archiviare, al termine della giornata lavorativa o nei casi di assenza prolungata, i dati cartacei nei contenitori previsti: se ciò non è possibile utilizzare le cassettiere delle scrivanie;
- spegnere il computer, al termine della giornata lavorativa o in caso di assenza prolungata, salvo che lo stesso debba essere lasciato acceso per altri motivi (es. un server di rete).

In particolare non dovrà:

- comunicare a terzi i dati personali di cui, per qualunque motivo, sono venuti a conoscenza nell' esercizio delle proprie mansioni, salvo diversa e motivata richiesta da parte del Titolare;
- diffondere, senza la preventiva autorizzazione del Titolare, i dati personali trattati;
- comunicare agli altri Incaricati ed a terzi, anche in modo indiretto, le proprie credenziali di autenticazione (UserName e Password).

L' incaricato prende atto che opererà sotto la diretta autorità del titolare o del responsabile, i quali avranno facoltà di revocare in ogni momento il presente incarico nonché, in caso di inadempimento a quanto in esso previsto, di revocare il mandato conferito all' incaricato per lo svolgimento delle attività, senza che questo ultimo possa avanzare eventuali pretese e fatto salvo il risarcimento del danno eventualmente subito.
Le revoche saranno effettuate con effetto immediato e senza obbligo di preavviso.
L'incaricato sottoscritto prende atto di quanto previsto nella presente nomina e dalla normativa vigente ed assume la qualifica di incaricato del trattamento.

_____ lì _____

Il Titolare del trattamento

_____

Per accettazione l' incaricato

_____

ALLEGATO 8

NOMINA DI INCARICATO MANUTENZIONE STRUMENTI ELETTRONICI

Il sottoscritto MARTINETTO ROBERTO SERGIO
in qualità di legale rappresentante della ditta BETA RICAMBI DI MARTINETTO ROBERTO SERGIO
con sede a TORINO
in C.SO GROSSETO 247/B CAP 10121

PREMESSO CHE

il Regolamento Europeo 2016/679, concernente la tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali fissa le modalità da adottare per detto trattamento ed individua i soggetti che, in relazione all'attività svolta, sono tenuti agli adempimenti previsti dallo stesso regolamento;
- il suddetto dregolamento prevede che "Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite. La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima";
- si intende procedere alla nomina degli incaricati dei trattamenti dei dati custoditi e gestiti da
MARTINETTO ROBERTO SERGIO

TUTTO CIO' PREMESSO
NOMINA
incaricato manutenzione strumenti elettronici il Sig/Sig.ra
MARTINETTO ROBERTO SERGIO

L'incaricato dovrà effettuare la manutenzione nel rispetto della normativa vigente e delle misure di sicurezza indicate dal citato Regolamento Europeo 2016/679 e quelle che successivamente verranno indicate in aggiornamento a quelle ivi previste.
L'incaricato dovrà, inoltre, rispettare le istruzioni impartite dal titolare o dal responsabile sia con il presente atto di nomina sia in seguito.

In particolare dovrà:
- 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.

L' incaricato si impegna, nel rispetto degli obblighi di riservatezza, a non divulgare e/o comunicare a terzi informazioni e dati dei quali sia venuto a conoscenza nel corso dell'intervento effettuato.

L' incaricato prende atto che opererà sotto la diretta autorità del titolare o del responsabile, i quali avranno facoltà di revocare in ogni momento il presente incarico nonché, in caso di inadempimento a quanto in esso previsto, di revocare il mandato conferito all' incaricato per lo svolgimento delle attività, senza che questo ultimo possa avanzare eventuali pretese e fatto salvo il risarcimento del danno eventualmente subito. Le revoche saranno effettuate con effetto immediato e senza obbligo di preavviso.
L'incaricato sottoscritto prende atto di quanto previsto nella presente nomina e dalla normativa vigente ed assume la
qualifica di incaricato della manutenzione degli strumenti elettronici.

_____ lì _____

Il Titolare del trattamento

_____

Per accettazione L'Incaricato

_____

incaricato manutenzione strumenti elettronici il Sig/Sig.ra **MARTINETTO ROBERTO SERGIO**

ALLEGATO 8

NOMINA DI INCARICATO DELLA CUSTODIA DELLE COPIE DI SICUREZZA

Il sottoscritto **MARTINETTO ROBERTO SERGIO**
in qualità di legale rappresentante della ditta BETA RICAMBI DI MARTINETTO ROBERTO SERGIO
con sede a TORINO
in C.SO GROSSETO 247/B CAP 10121

PREMESSO CHE

il Regolamento Europeo 2016/679, concernente la tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali fissa le modalità da adottare per detto trattamento ed individua i soggetti che, in relazione all'attività svolta, sono tenuti agli adempimenti previsti dallo stesso regolamento;
- il suddetto regolamento prevede che "Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite. La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima";
- si intende procedere alla nomina degli incaricati dei trattamenti dei dati custoditi e gestiti da
MARTINETTO ROBERTO SERGIO

TUTTO CIO' PREMESSO
NOMINA
incaricato delle copie di back-up dei dati il Sig/Sig.ra
MARTINETTO ROBERTO SERGIO

L' incaricato delle copie di sicurezza delle banche dati ha il compito di:

- 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 almeno settimanale;
- 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;
- 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, l'incaricato dovrà:

- 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.

L' incaricato prende atto che opererà sotto la diretta autorità del titolare o del responsabile, i quali avranno facoltà di revocare in ogni momento il presente incarico nonché, in caso di inadempimento a quanto in esso previsto, di revocare il mandato conferito all' incaricato per lo svolgimento delle attività, senza che questo ultimo possa avanzare eventuali pretese e fatto salvo il risarcimento del danno eventualmente subito. Le revoche saranno effettuate con effetto immediato e senza obbligo di preavviso.
L'incaricato sottoscritto prende atto di quanto previsto nella presente nomina e dalla normativa vigente ed assume la qualifica di incaricato del trattamento.

_____ lì _____

Il Titolare del trattamento

_____

Per accettazione
L' Incaricato

_____

ALLEGATO 8

NOMINA DI INCARICATO DELLA CUSTODIA CREDENZIALI DI AUTENTICAZIONE

Il sottoscritto MARTINETTO ROBERTO SERGIO
in qualità di legale rappresentante della ditta BETA RICAMBI DI MARTINETTO ROBERTO SERGIO
con sede a TORINO
in C.SO GROSSETO 247/B CAP 10121

PREMESSO CHE

il Regolamento Europeo 2016/679, concernente la tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali fissa le modalità da adottare per detto trattamento ed individua i soggetti che, in relazione all'attività svolta, sono tenuti agli adempimenti previsti dallo stesso regolamento;
- il suddetto regolamento prevede che "Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite. La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima";
- si intende procedere alla nomina degli incaricati dei trattamenti dei dati custoditi e gestiti da
MARTINETTO ROBERTO SERGIO

TUTTO CIO' PREMESSO
NOMINA
incaricato della custodia delle credenziali di autenticazione degli operatori con accesso ai dati il Sig/Sig.ra
MARTINETTO ROBERTO SERGIO

L' incaricato della custodia delle credenziali di autenticazione ha il compito di:
- 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 al cui interno 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.

L' incaricato prende atto che opererà sotto la diretta autorità del titolare o del responsabile, i quali avranno facoltà di revocare in ogni momento il presente incarico nonché, in caso di inadempimento a quanto in esso previsto, di revocare il mandato conferito all' incaricato per lo svolgimento delle attività, senza che questo ultimo possa avanzare eventuali pretese e fatto salvo il risarcimento del danno eventualmente subito. Le revoche saranno effettuate con effetto immediato e senza obbligo di preavviso.
L'incaricato sottoscritto prende atto di quanto previsto nella presente nomina e dalla normativa vigente ed assume la qualifica di incaricato del trattamento.

_____ lì _____

Il Titolare del trattamento
_____

Per accettazione
L' incaricato
_____

ALLEGATO 8

NOMINA DI RESPONSABILE DEL TRATTAMENTO DI DATI PERSONALI

Il sottoscritto MARTINETTO ROBERTO SERGIO
in qualità di legale rappresentante della ditta BETA RICAMBI DI MARTINETTO ROBERTO SERGIO
con sede a TORINO
in C.SO GROSSETO 247/B CAP 10121

NOMINA

Responsabile del trattamento dei dati personali il Sig./ La Sig.ra

MARTINETTO ROBERTO SERGIO

in conformità al Regolamento Europeo 2016/679 con i seguenti compiti ed attribuzioni:
- 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;

a tale scopo provvede a:
- individuare in forma scritta gli incaricati al trattamento dei dati;
- predisporre le misure minime di sicurezza ai sensi del Regolamento Europeo 2016/679;
- elaborare il "Manuale della Privacy";
-vigilare sulla corretta osservanza degli obblighi di legge e dei diritti riconosciuti dalla legge agli interessati;
- formare il personale relativamente alle disposizioni previste dal Regolamento Europeo 2016/679;
- 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;
- custodire e conservare i supporti utilizzati per le copie dei dati;
- 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 in materia di dati personali;
- di dare periodicamente, e comunque almeno annualmente, le istruzioni adeguate agli incaricati del trattamento effettuato con strumenti elettronici e non, e verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione degli incaricati del trattamento dei dati personali.

Il Responsabile del trattamento dei dati personali, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più Responsabili con il compito di affiancarlo nello svolgimento delle attività ed eventualmente con la possibilità di individuare, nominare e incaricare per iscritto gli Incaricati del trattamento dei dati personali.

Il "Responsabile del Trattamento dei dati personali " dichiara di accettare l'incarico e i compiti che gli sono affidati e di essere a conoscenza di quanto stabilito dal Codice in materia di dati personali, e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

_____lì,_____

Il Titolare
_____

Per accettazione
Il Responsabile del Trattamento

_____

ALLEGATO 9

LEGENDA DELLA MAPPATURA DEL RISCHIO

Tipo mancanza	Probabilità	Pericolo	Rischio
Eventi distruttivi, naturali o artificiali, nonché dolosi, accidentali o dovuti ad incuria.	1	4	4
Danni provocati da un possibile guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.)	2	2	4
Responsabile supporti informatici Esterno alla Ditta con accesso alle banche dati	1	2	2
Sistema di Identificazione assente	4	4	16
Password con meno di 8 caratteri alfanumerici	2	2	4
Password che riconducono all' utente o alla ditta	1	2	2
Mancata impostazione scadenza Password	2	4	8
Scadenza Password non conforme alle MMS	2	3	6
Assenza di test Firewall	1	2	2
Mancata impostazione sistema di Stand-by	1	2	2

Mancata rimozione delle autorizzazioni non utilizzare da lungo tempo	2	4	8
Assenza di un gruppo di continuità	2	3	6
Assenza programma Antivirus senza connessione ad internet	4	3	12
Assenza programma Antivirus con connessione ad Internet	4	4	16
Assenza Firewall con connessione ad Internet 64K	1	4	4
Assenza Firewall con connessione ad Internet ISDN	2	4	8
Assenza Firewall con connessione ad Internet ADSL	3	4	12
Assenza Firewall con connessione ad Internet HDSL o superiori	4	4	16
Assenza di controlli su materiale proveniente dall' esterno	2	2	4
Assenza di sistema di Backup con gruppo di Continuità installato	2	4	8
Assenza di sistema di Backup senza gruppo di Continuità installato	3	4	12
Accessibilità dati sensibili a soggetti non autorizzati	3	4	12

Possibile sottrazione di credenziali di autenticazione	3	4	12
Carenza di consapevolezza, disattenzione o incuria da parte del personale incaricato	3	3	9
Errore materiale da parte del personale incaricato	1	4	4
Accessi non autorizzati a locali e reparti dove vengono custoditi dati personali	2	4	8

Dati relativi all' identità genetica trattati in locali non protetti	2	4	8
Accesso non autorizzato ai locali dove sono contenuti dati genetici	3	4	12
Mancata protezione dei dati genetici durante trasporto esterno	2	4	8
Mancata protezione dati genetici durante trasferimento in formato elettronico	2	4	8
Prove di ripristino dei dati non effettuate	2	4	8
Mancata conservazione delle copie delle credenziali di autenticazione	2	3	6

Mancata separazione tra dati identificativi e dati sensibili su banche dati trattate con sistemi elettronici	2	3	6
Tempi di ripristino dei dati (sensibili e giudiziari) in caso di danneggiamento degli stessi o degli strumenti elettronici non compatibili alle MMS (maggiori di 7 giorni)	2	4	8

Riutilizzo di supporti rimovibili contenenti dati sensibili o giudiziari da parte di altri incaricati non autorizzati.	2	4	8
Protocollo HTTPS - HyperText Transfer Protocol Secure (HTTPS) protocollo per la comunicazione su Internet che protegge l'integrità e la riservatezza dei dati scambiati tra i computer e i siti	2	4	8
Utilizzo cookies - Il cookie è un token digitale, ovvero un breve pacchetto di dati scambiato tra programmi in comunicazione fra loro. I cookie web sono usati dai server web per poter riconoscere i browser durante comunicazioni con il protocollo HTTP usato per la navigazione web.	3	4	12
Anonimizzazione IP Google Analytics - La funzione di anonimizzazione IP in Analytics imposta l'ultimo ottetto di indirizzi IP dell'utente IPv4 e gli ultimi 80 bit degli indirizzi IPv6 su zero in memoria subito dopo l'invio alla rete di raccolta di Analytics; in questo caso l'indirizzo IP completo non è mai scritto su disco.	2	4	8
Condivisione dati Google Analytics - Per impedire l’ incrocio dei dati con altri servizi Google, occorre accedere alle impostazioni dell’ account Analytics e deselezionare le opzioni di condivisione dei dati.	2	2	4
Sistema di videosorveglianza	4	4	16

ALLEGATO 10

PROGRAMMA DI INTERVENTO

Verificare di aver fornito informativa ai soggetti di cui si trattano i dati.
Verificare di aver ottenuto il consenso al trattamento dei dati nei casi previsti.

Misure non adottate	Azione correttiva	Rischio	Tempi di adeguamento	Funzione responsabile dell'adeguamento
Eventi distruttivi, naturali o artificiali, nonché dolosi, accidentali o dovuti ad incuria.	Formare il personale su disciplina, rischi connessi e misure da adottare per evitare la perdita accidentale dei dati personali	4	Max 6 mesi	Titolare del trattamento/Responsabile del trattamento
Danni provocati da un possibile guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.)	Formare il personale su disciplina, rischi connessi e misure da adottare per evitare la perdita accidentale dei dati personali	4	Max 6 mesi	Titolare del trattamento/Responsabile del trattamento
Responsabile supporti informatici Esterno alla Ditta con accesso alle banche dati	Limitare libertà di accesso a collaboratori esterni	2	Da programmare	Titolare del trattamento
Sistema di Identificazione assente	Impostare un sistema di identificazione	16	Immediato	Titolare o Responsabile del trattamento/incaricato della manutenzione degli strumenti elettronici
Password che riconducono all'utente o alla ditta	Cambiare PASSWORD	2	Da programmare	Titolare o Responsabile del trattamento / Incaricati del trattamento
test firewall	Richiedere un test del firewall	2	Da programmare	Titolare o Responsabile del trattamento / Incaricato della manutenzione degli strumenti elettronici
Mancata rimozione	Stabilire scadenze per	8	Immediato	Titolare o Responsabile del

delle autorizzazioni non utilizzate da lungo tempo	autorizzazioni non utilizzate			trattamento / Incaricato della manutenzione degli strumenti elettronici
Assenza di un gruppo di continuità	Installare un gruppo di continuità	6	Max 3 mesi	Titolare o Responsabile del trattamento / Incaricato della manutenzione degli strumenti elettronici
In caso di protocollo HTTPS – HyperText Transfer Protocol Secure (HTTPS)	Attivare Protocollo	8	Max 3 mesi	Titolare o Responsabile del trattamento
In caso di utilizzo cookies	Inserire nel sito l'informativa per l'uso dei cookies	12	Immediato	Titolare o Responsabile del trattamento
In caso di anonimizzazione IP Google Analytics	Attivare funzione	8	Immediato	Titolare o Responsabile del trattamento
In caso di condivisione dati Google Analytics	Deselezionare le opzioni di condivisione dei dati.	4	Max 3 mesi	Titolare o Responsabile del trattamento

In caso di sistema di videosorveglianza	Richiedere l' accordo con le rappresentanze sindacali unitarie o aziendali oppure in caso di assenza di Rappresentanze sindacali richiedere l' autorizzazione preventiva, per l' installazione delle apparecchiature di videosorveglianza, all' Ispettorato territoriale del lavoro	16	Immediato	Titolare o Responsabile del trattamento
In caso di sistema di videosorveglianza	Affiggere appositi cartelli informativi e di avvertimento al pubblico e sono esposti sia all' esterno che all' interno dei locali soggetti a videosorveglianza	16	Immediato	Titolare o Responsabile del trattamento
In caso di sistema di videosorveglianza	Predisporre un' informativa ed è conforme alla normativa vigente	16	Immediato	Titolare o Responsabile del trattamento
Assenza di controlli su materiale proveniente dall'esterno	Controllare il materiale proveniente dall'esterno	4	Max 6 mesi	Titolare del trattamento/Responsabile del trattamento/Incaricati del trattamento
Assenza di back up	Impostare un sistema di back up	8	Immediato	Titolare o Responsabile del trattamento / Incaricato della manutenzione degli strumenti elettronici

Possibile sottrazione di credenziali di autenticazione	Conservare le copie delle credenziali di autenticazione in luogo non accessibile	12	Immediato	Titolare del trattamento/Responsabile del trattamento/Incaricati della custodia delle copie delle credenziali
Errore materiale del personale incaricato	Formare il personale su disciplina, rischi connessi e misure da adottare per evitare la perdita accidentale dei dati personali	4	Max 6 mesi	Titolare del trattamento/Responsabile del trattamento
Accessi non autorizzati a locali e reparti dove vengono custoditi dati personali	Interdire l'accessibilità ai locali e reparti dove vengono custoditi dati personali, ai soggetti non autorizzati	8	Immediato	Titolare del trattamento/Responsabile del trattamento
Prove di ripristino dei dati non effettuate	Effettuare periodiche prove di ripristino dei dati	8	Immediato	Titolare del trattamento/Responsabile del trattamento
Tempi di ripristino dei dati (sensibili e giudiziari) in caso di danneggiamento degli stessi o degli strumenti elettronici non compatibili alle MMS (maggiori di 7 giorni)	Adottare misure idonee per garantire il ripristo dell'accesso ai dati sensibili o giudiziari trattati con strumenti elettronici in tempi non superiori ai 7 giorni.	8	Immediato	Titolare o Responsabile del trattamento/Incaricato della manutenzione degli strumenti elettronici

ALLEGATO 10

MISURE DI SICUREZZA IN ESSERE

Tipologia di Rischio	Misure in essere	Rischio	Note
Sottrazione delle credenziali di autenticazione	Sistema di autenticazione con numero di caratteri pari o superiore a 8	1	
Accessi non autorizzati	Id e password aggiornati periodicamente	1	
Accessi non autorizzati	Presenza di uno screen-saver	1	
Perdita dei dati	Presenza di un antivirus	1	
Accessi non autorizzati	Presenza di un firewall	1	
Sottrazione delle credenziali di autenticazione	Le copie delle credenziali di autenticazione sono custodite diligentemente, in luogo sicuro e da personale preventivamente incaricato. È garantita la segretezza delle copie delle credenziali di autenticazione.	1	
Perdita dei dati Accessi non autorizzati	Il personale incaricato del trattamento è stato adeguatamente formato sulla disciplina di protezione dei dati personali, sui rischi che incombono sui dati e sulle misure disponibili per prevenire eventi dannosi.	1	

ALLEGATO 11

REGISTRO DELLA FORMAZIONE

FORMAZIONE EFFETTUATA	
Argomento:	
DATA	

NOME E COGNOME DEI PRESENTI	FIRMA DI PRESENZA

ALLEGATO 12

TRATTAMENTO DEI DATI AFFIDATI ALL'ESTERNO (outsourcing)

Descrizione attività	Responsabilità/Incarico	Nominativo	Banche dati affidate
0		0	UFFICIO
0		0	0
0		0	0

SCHEDE AD UTILIZZO DELL'AZIENDA
PER IL CONSENSO DEL TRATTAMENTO DEI DATI
Da sottoporre a tutti i soggetti compresi i minori di età.

LA SCHEDA:

Informativa al trattamento dei dati personali.

Da esporre presso il locale in modo visibile

Il Sottoscritto	
Codice Fiscale	
Nato a	Il __/__/____
Residente a	Via
Telefono	

in qualità di titolare della responsabilità genitoriale del minore

Cognome Nome:	
Codice Fiscale	
Nato a	Il __/__/____
Residente a	Via
Telefono	

ACCONSENTE

ai sensi e per gli effetti del Regolamento Europeo (EU) 2016/679 agli artt. 6, 7, 8, 12, 13 e 14, con la sottoscrizione del presente modulo, al trattamento dei dati personali per la seguente finalità

FINALITA'

Mailing list per aggiornamenti attività, comunicazioni'

□ DA IL CONSENSO
□ NEGA IL CONSENSO Firma _____

solo ed esclusivamente da BETA RICAMBI DI MARTINETTO ROBERTO SERGIO

Senza il consenso espresso del soggetto interessato (ai sensi dell'art. 7 del Reg. UE 2016/679) non si potrà fornire all'interessato i servizi e/o i prodotti richiesti, in tutto o in parte.
I dati personali non sono diffusi a società o persone esterne.

Titolare del trattamento
Il Titolare del trattamento dei dati è **BETA RICAMBI DI MARTINETTO ROBERTO SERGIO**
C.SO GROSSETO 247/B CAP 10121-TORINO-

in ogni momento potrà esercitare i Suoi diritti nei confronti del Titolare del trattamento, ai sensi degli artt. 12, 13, 14, 15, 16,17, 18 e 20 del Reg. UE 2016/679, per avere informazioni. Accesso, portabilità, rettifica, cancellazione o limitazione sul trattamento dei Suoi dati.

Letto, confermato e sottoscritto

_____ Li _____

_____
Firma del dichiarante
(per esteso e leggibile)

CONSENSO AL TRATTAMENTO DEI DATI PERSONALI

BETA RICAMBI DI MARTINETTO ROBERTO SERGIO

Il Sottoscritto	
Codice Fiscale	
Nato a	Il __/__/____
Residente a	Via
Telefono	

Preso atto dell'informativa e dei diritti a me riservati in tema di trattamento dei dati personali, ai sensi del Regolamento Europeo 2016/679, al trattamento dei miei dati personali ad opera dei soggetti indicati nella predetta informativa, per le finalità indicate e nei limiti di cui alla stessa.

□ DA IL CONSENSO
□ NEGA IL CONSENSO Firma _____

Per quanto riguarda la comunicazione dei miei dati personali a soggetti che svolgono attività funzionalmente collegate all'esecuzione del servizio, quali: - attività di elaborazione, registrazione e archiviazione dei dati, - attività bancaria e finanziaria.

□ DA IL CONSENSO
□ NEGA IL CONSENSO Firma _____

Per quanto riguarda la comunicazione dei dati personali a soggetti che svolgono attività d'informazione commerciale.

□ DA IL CONSENSO
□ NEGA IL CONSENSO Firma _____

Rimane fermo che il consenso sopra espresso è condizionato al rispetto delle disposizioni della vigente normativa in materia di protezione dei dati personali (Regolamento Europeo 2016/679).

Ai sensi del Regolamento Europeo 2016/679 desideriamo informarVi che:

- i dati personali da Voi forniti o acquisiti nell'ambito dei rapporti contrattuali con Voi intercorrenti, vengono utilizzati allo scopo di:
  NON E' PRESENTE NESSUNA FINALITA'

- in occasione di tali trattamenti è possibile venire a conoscenza di dati che il Regolamento Europeo 2016/679 definisce "sensibili".

- il trattamento dei dati conferiti avviene nel rispetto delle norme vigenti, a mezzo di strumenti CARTACEI ED INFORMATICI idonei a tutelare la Vostra sicurezza e riservatezza, nel rispetto delle misure minime previste dal Regolamento Europeo 2016/679. Tale trattamento consiste nella raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, duplicazione, estrazione, selezione, raffronto, utilizzo, cancellazione e distruzione dei dati stessi;

- il conferimento dei dati personali richiesti è obbligatorio

- una loro mancata o parziale comunicazione impedirebbe di instaurare rapporti con la scrivente in quanto risulterebbe impossibile adempiere al contratto;

- i dati forniti o acquisiti nel corso del rapporto contrattuale potranno essere comunicati a soggetti esterni che svolgono specifici incarichi per conto dell'azienda

- non è prevista la possibilità di diffondere i vostri dati all'esterno

BETA RICAMBI DI MARTINETTO ROBERTO SERGIO
C.SO GROSSETO 247/B CAP 10121 -TORINO -
è titolare del trattamento
MARTINETTO ROBERTO SERGIO
è responsabile del Trattamento dei Dati

- i dati conferiti saranno trattati da personale incaricato nominato direttamente dal Responsabile del Trattamento

- i dati personali non sono trasferiti all'estero

- i dati personali sono conservati per una durata massima di cinque anni e/o fina alla conclusione del rapporto contrattuale.

Vi informiamo altresì che Il Regolamento Europeo 2016/679 riconosce all'interessato il diritto di:

- chiedere la conferma dell'esistenza dei dati personali che lo riguardano,
- avere informazioni sul trattamento dei medesimi,
- richiederne l'aggiornamento, la rettifica, l'integrazione, la cancellazione, la trasformazione in forma anonima e il blocco dei dati personali, trattati in violazione di legge,
- di opporsi al trattamento per motivi legittimi.
- di opporsi alla sottoscrizione di eventuali consensi al trattamento, finalizzati a gestioni diverse da quanto indicato in informativa.

Tale diritto può essere esercitato rivolgendo un'istanza al titolare o al Responsabile del trattamento Incaricati.

Istruzioni per l'utilizzo della documentazione in materia di trattamento dei dati personali

Spettabile **BETA RICAMBI DI MARTINETTO ROBERTO SERGIO**

siamo lieti di inviarVi la documentazione redatta al fine di adeguare la Vostra struttura alle disposizioni dettate dal Regolamento Europeo 2016/679.

Elenco dei documenti consegnati
* Manuale Privacy;
* Allegati al Manuale Privacy:
  - ° Allegato 1 – Dati dell'azienda;
  - ° Allegato 2 – Tipo trattamento dati personali;
  - ° Allegato 3 – Definizione dei luoghi di trattamento dei dati;
  - ° Allegato 4 – Archivi informatici e cartacei;
  - ° Allegato 5 – Banche dati;
  - ° Allegato 6 – Dati sanitari (presente solo per organismi esercenti attività sanitarie);
  - ° Allegato 7 – Piano di formazione;
  - ° Allegato 8 – Nomine Responsabili ed Incaricati;
  - ° Allegato 9 – Leggenda della mappatura del rischio;
  - ° Allegato 10 – Programma di intervento e Misure di sicurezza in essere;
  - ° Allegato 11 – Registro della formazione;
  - ° Allegato 12 – Trattamento dei dati affidati all'esterno.
* Informativa per il trattamento dei dati personali;
* Consenso al trattamento dei dati personali e sensibili (solo se previsto dalla normativa cogente);
* Corso Privacy da utilizzare come materiale didattico nella formazione interna Istruzioni per l'utilizzo della documentazione

Manuale Privacy
Il documento deve essere datato e firmato per approvazione da parte del Titolare del trattamento (al capitolo 12).
Questo deve essere conservato presso gli uffici della Vostra struttura a disposizione di Responsabili ed Incaricati nonché dagli enti preposti per i controlli (Polizia di Stato, Guardia di Finanza).

Allegati
Gli allegati (da 1 a 12), fanno parte integrante del Manuale Privacy, tutti gli allegati che la costituiscono devono essere conservati insieme con il Manuale Privacy medesimo. Presso la sua posta elettronica sarà inviato il file completo del "REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO.", per meglio completare la sua informazione inerente alla materia.

Informativa
L'informativa deve essere resa nota a tutti i soggetti interessati al trattamento (clienti, utenti, personale, fornitori e qualsiasi altra "persona fisica, giuridica, ente o associazione cui si riferiscono i dati personali", come definito dal Regolamento Europeo.
Le modalità per rendere nota l'informativa sono molteplici: consegna/invio del documento ad ogni soggetto interessato, affissione in bacheche all'interno degli uffici, pubblicazione su sito internet, etc.)

Consenso (solo se previsto dalla normativa cogente)
Il consenso, se previsto dalla legge in relazione alla tipologia dei dati di cui si è in possesso e dei trattamenti su di essi effettuati, deve essere compilato in ogni sua parte e sottoscritto dal soggetto interessato e conservato a cura del Titolare del trattamento.
Per ogni ulteriore informazione o delucidazione non esitate a contattarci ai recapiti di cui siete in possesso.

Cordiali saluti