

# Modello Organizzativo Privacy

Il presente documento è stato redatto in base alle ultime disposizioni legislative finalizzate all'allineamento dei principi sanciti nel Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

## Definizioni Principali Normativa Privacy

**Titolare del Trattamento:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

**Responsabile del Trattamento:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

**Addetti al Trattamento:** le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

**Interessato:** la persona fisica a cui si riferiscono i dati personali (tutti noi siamo interessati).

**Destinatario:** la persona fisica o giuridica, l'autorità pubblica; il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri, non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.

**Dato personale:** qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"). Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

**Dato sensibile:** 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 rilevare lo stato di salute e la vita sessuale.

**Dato giudiziario:** i dati personali idonei a rivelare informazioni 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.

**Dati genetici:** i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia, sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.

**Dati biometrici:** dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

**Dati relativi alla salute:** i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

**Trattamento Dati:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

## **Principi Generali Adottati dall'Organizzazione**

La Bolamì srl è tenuta a garantire 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.

## **Obblighi di sicurezza**

La Bolamì srl è tenuta a garantire che i dati personali oggetto di trattamento siano custoditi e controllati, anche in relazione alle conoscenze acquisite in base allo stato dell'arte e all'avanzamento tecnologico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo - mediante l'adozione di idonee di sicurezza - 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.

## **Misure di Sicurezza Idonee**

La Bolamì srl è tenuta ad adottare un complesso di misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza per assicurare un livello idoneo di protezione dei dati personali, sia nel caso di trattamenti con strumenti elettronici sia nel caso di trattamenti senza l'ausilio di strumenti elettronici.

## **Dati Generali**

<b>Titolare del trattamento</b>	<b>Stefano Sarti</b>
---------------------------------	----------------------

## **Finalità del trattamento**

Comunicazione con clienti, fornitori, soci, terzi o pazienti necessari alla reperibilità, alla corrispondenza con gli stessi o richiesti a fini fiscali

Gestione del rapporto con i collaboratori

Gestione del rapporto contrattuale con il cliente

Gestione del rapporto contrattuale con utenti di servizi

Gestione del rapporto di lavoro

Gestione del rapporto di lavoro con dipendenti

Gestione rapporti pre-contrattuali (invio informazioni)

Indagini di mercato

Inserimento nel DB per rapporto continuativo con l'interessato

Rapporto di lavoro, corrispondenza o richieste a fini fiscali e previdenziali o dati di natura bancaria

Relative ad adempimenti fiscali o contabili

Risoluzione di problemi o reclami del cliente (inbound call)

Servizi basati sulla geo-localizzazione

Statistiche

Svolgimento della propria attività

Tutela del legittimo interesse del Titolare

### **Tipo di dati Trattati**

I dati trattati sono: Amministrativo, Contabili, Bancari, Finanziari, Comuni, Dati personali, Fiscali, Previdenziali e sul lavoro

### **Censimento dei dati trattati**

Tipo banca dati	Cedolini buste paga,CUD dipendenti,Dichiarazione dei redditi
Finalità perseguita	Gestione del rapporto di lavoro con dipendenti
Categoria di interessati	Dipendenti

Tipo banca dati	Azienda corrispondenza,Controllo documenti d'identità,Documenti per adempimenti fiscali
Finalità perseguita	Gestione del rapporto con i collaboratori
Categoria di interessati	Collaboratori

Tipo banca dati	Anagrafica clienti,Anagrafica fornitori,Azienda corrispondenza,Contratti clienti,Contratto fornitori,Controllo documenti d'identità,Documenti per adempimenti fiscali,Fatture acquisto fornitori,Fatture di vendita dei clienti,Portali clienti,Rubrica indirizzi di posta elettronica,Rubrica indirizzi e numeri di telefono
Finalità perseguita	Comunicazione con clienti, fornitori, soci, terzi o pazienti necessari alla reperibilità, alla corrispondenza con gli stessi o richieste a fini fiscali
Categoria di interessati	Clienti,Fornitori

Tipo banca dati	Accessi PayPal,Accessi remote banking,Anagrafica clienti,Fatture acquisto fornitori,Rubrica indirizzi di posta elettronica,Rubrica indirizzi e numeri di telefono
Finalità perseguita	Gestione del rapporto contrattuale con utenti di servizi
Categoria di interessati	Collaboratori,Dipendenti,Fornitori

Tipo banca dati	Azienda corrispondenza, CUD dipendenti,Dichiarazione dei redditi,Documenti per adempimenti fiscali contribuenti,Rubrica indirizzi di posta elettronica,Rubrica indirizzi e numeri di telefono
Finalità perseguita	Gestione del rapporto di lavoro
Categoria di interessati	Collaboratori,Dipendenti

Tipo banca dati	Accessi PayPal,Accessi remote banking,Anagrafica clienti,Bilanci di contabilità,Cedolini buste paga,CUD dipendenti,Documenti per adempimenti fiscali,Fatture acquisto fornitori,Fatture di vendita dei clienti,Portali clienti,Rubrica indirizzi di posta elettronica,Rubrica indirizzi e numeri di telefono
Finalità perseguita	Tutela del legittimo interesse del Titolare
Categoria di interessati	Clienti,Collaboratori,Dipendenti,Fornitori

Tipo banca dati	Anagrafica clienti,Anagrafica fornitori,Anagrafica incaricati,Cedolini buste paga,Contratto fornitori,CUD dipendenti,Documenti per adempimenti fiscali,Fatture acquisto fornitori,Fatture di vendita dei clienti
Finalità perseguita	Inserimento nel DB per rapporto continuativo con l'interessato
Categoria di interessati	Clienti,Collaboratori,Dipendenti,Fornitori

Tipo banca dati	Accessi PayPal,Accessi remote banking,Anagrafica fornitori,Cedolini buste paga,Controllo documenti d'identità,CUD dipendenti,Documenti per adempimenti fiscali
Finalità perseguita	Rapporto di lavoro, corrispondenza o richiesti a fini fiscali e previdenziali o dati di natura bancaria
Categoria di interessati	Collaboratori,Dipendenti,Fornitori

Tipo banca dati	Anagrafica clienti,Azienda corrispondenza,Fatture di vendita dei clienti,Rubrica indirizzi di posta elettronica,Rubrica indirizzi e numeri di telefono
Finalità perseguita	Risoluzione di problemi o reclami del cliente (inbound call)
Categoria di interessati	Clienti

Tipo banca dati	Accessi PayPal,Accessi remote banking,Anagrafica clienti,Anagrafica fornitori,Anagrafica incaricati,Anagrafica Outsourcing,Azienda corrispondenza,Bilanci di contabilità,Cedolini buste paga,Contratti clienti,Contratto fornitori,Controllo documenti d'identità,CUD dipendenti,Dichiarazione dei redditi,Documenti per adempimenti fiscali,Fatture acquisto fornitori,Fatture di vendita dei clienti,Portali clienti,Rubrica indirizzi di posta elettronica,Rubrica indirizzi e numeri di telefono
Finalità perseguita	Svolgimento della propria attività
Categoria di interessati	Clienti,Collaboratori,Dipendenti,Fornitori

Tipo banca dati	Accessi PayPal,Accessi remote banking,Anagrafica clienti,Anagrafica controllo accessi,Anagrafica fornitori,Anagrafica incaricati,Anagrafica Outsourcing,Azienda corrispondenza,Bilanci di contabilità,Cedolini buste paga,Contratti clienti,Contratto fornitori,Controllo documenti d'identità,CUD dipendenti,Dichiarazione dei redditi,Documenti per adempimenti fiscali,Fatture acquisto fornitori,Fatture di vendita dei clienti,Portali clienti,Rubrica indirizzi di posta elettronica,Rubrica indirizzi e numeri di telefono
Finalità perseguita	Svolgimento della propria attività
Categoria di interessati	Clienti,Collaboratori,Dipendenti,Fornitori

Tipo banca dati	Portali clienti,Rubrica indirizzi di posta elettronica,Rubrica indirizzi e numeri di telefono
Finalità perseguita	Indagini di mercato
Categoria di interessati	Clienti,Collaboratori,Dipendenti

## Trattamenti affidati all'esterno

Il titolare del trattamento, relativamente ad alcuni trattamenti di dati, ha affidato la loro gestione a soggetti esterni designandoli formalmente con apposita lettera di nomina.

Di seguito sono sintetizzati i criteri e gli impegni assunti dalle parti esterne all'organizzazione per l'adozione delle misure di sicurezza, affinché venga garantito un adeguato trattamento.

Banca dati affidata in outsourcing	Anagrafica clienti, Anagrafica fornitori, Anagrafica incaricati, Azienda corrispondenza, Documenti per adempimenti fiscali, Portali clienti, Rubrica indirizzi di posta elettronica, Rubrica indirizzi e numeri di telefono
Soggetto esterno	Alessia Samperi (Social Media Management)
Attività prestata	Consulenza informatica
Descrizione dei criteri e degli impegni assunti per l'adozione delle misure minime di sicurezza (tipo di dichiarazione che la società a cui viene affidato il trattamento rilascia o il tipo di impegno assunto anche su base contrattuale)	
<p>Trattamento di dati ai soli fini dell'espletamento dell'incarico ricevuto</p> <p>Adempimenti degli obblighi previsti dal Codice per la protezione dei dati personali</p> <p>Rispetto delle istruzioni specifiche ricevute dal titolare del trattamento</p> <p>Impegno a relazionare periodicamente sulle misure di sicurezza adottate – anche mediante eventuali questionari e liste di controllo – e ad informare immediatamente il titolare del trattamento in caso di situazioni anomale o di emergenze</p> <p>Trattamento di dati ai soli fini dell'espletamento dell'incarico ricevuto</p>	

Banca dati affidata in outsourcing	Anagrafica clienti, Anagrafica contribuenti, Anagrafica fornitori, Bilanci di contabilità, Contratti clienti, Contratto fornitori, Dichiarazione dei redditi, Documenti per adempimenti fiscali, Fatture acquisto fornitori
Soggetto esterno	Francesco Toschi (Commercialista)
Attività prestata	Consulenza fiscale/tributaria
Descrizione dei criteri e degli impegni assunti per l'adozione delle misure minime di sicurezza (tipo di dichiarazione che la società a cui viene affidato il trattamento rilascia o il tipo di impegno assunto anche su base contrattuale)	
<p>Trattamento di dati ai soli fini dell'espletamento dell'incarico ricevuto</p> <p>Adempimenti degli obblighi previsti dal Codice per la protezione dei dati personali</p> <p>Rispetto delle istruzioni specifiche ricevute dal titolare del trattamento</p> <p>Impegno a relazionare periodicamente sulle misure di sicurezza adottate – anche mediante eventuali questionari e liste di controllo – e ad informare immediatamente il titolare del trattamento in caso di situazioni anomale o di emergenze</p> <p>Trattamento di dati ai soli fini dell'espletamento dell'incarico ricevuto</p>	

Banca dati affidata in outsourcing	Cedolini buste paga, CUD dipendenti, Documenti per adempimenti fiscali
Soggetto esterno	Lara Giovannini (Consulente del lavoro)
Attività prestata	Consulente del lavoro
Descrizione dei criteri e degli impegni assunti per l'adozione delle misure minime di sicurezza (tipo di dichiarazione che la società a cui viene affidato il trattamento rilascia o il tipo di impegno assunto anche su base contrattuale)	

Trattamento di dati ai soli fini dell'espletamento dell'incarico ricevuto  
 Adempimenti degli obblighi previsti dal Codice per la protezione dei dati personali  
 Rispetto delle istruzioni specifiche ricevute dal titolare del trattamento  
 Impegno a relazionare periodicamente sulle misure di sicurezza adottate – anche mediante eventuali questionari e liste di controllo – e ad informare immediatamente il titolare del trattamento in caso di situazioni anomale o di emergenze  
 Trattamento di dati ai soli fini dell'espletamento dell'incarico ricevuto

Banca dati affidata in outsourcing	Accessi PayPal, Anagrafica clienti, Azienda corrispondenza, Contratti clienti, Fatture di vendita dei clienti, Portali clienti, Rubrica indirizzi di posta elettronica, Rubrica indirizzi e numeri di telefono
Soggetto esterno	Riccardo Armari (Digital Marketing Specialist)
Attività prestata	Consulenza informatica
Descrizione dei criteri e degli impegni assunti per l'adozione delle misure minime di sicurezza (tipo di dichiarazione che la società a cui viene affidato il trattamento rilascia o il tipo di impegno assunto anche su base contrattuale)	
<p>Trattamento di dati ai soli fini dell'espletamento dell'incarico ricevuto          Adempimenti degli obblighi previsti dal Codice per la protezione dei dati personali          Rispetto delle istruzioni specifiche ricevute dal titolare del trattamento          Impegno a relazionare periodicamente sulle misure di sicurezza adottate – anche mediante eventuali questionari e liste di controllo – e ad informare immediatamente il titolare del trattamento in caso di situazioni anomale o di emergenze          Trattamento di dati ai soli fini dell'espletamento dell'incarico ricevuto</p>	

Adempimento degli obblighi previsti dal Codice per la protezione dei dati personali.

Rispetto delle istruzioni specifiche ricevute dal titolare del trattamento.

Impegno a relazionare periodicamente sulle misure di sicurezza adottate – anche mediante eventuali questionari e liste di controllo – e ad informare immediatamente il titolare del trattamento in caso di situazioni anomale o di emergenze.

Trattamento di dati ai soli fini dell'espletamento dell'incarico ricevuto.

Adempimento degli obblighi previsti dal Codice per la protezione dei dati personali.

Rispetto delle istruzioni specifiche ricevute dal titolare del trattamento.

Impegno a relazionare periodicamente sulle misure di sicurezza adottate— anche mediante eventuali questionari e liste di controllo — e ad informare immediatamente il titolare del trattamento in caso di situazioni anomale o di emergenze.

## **Procedura per l'accesso, la conservazione e la cancellazione**

### ***Accesso ai dati***

La Bolami srl ha identificato come categorie di interessati le seguenti categorie:

Dipendenti

Collaboratori

Clienti,Fornitori

Collaboratori,Dipendenti,Fornitori

Collaboratori,Dipendenti

Clienti,Collaboratori,Dipendenti,Fornitori

Clienti

Clienti,Collaboratori,Dipendenti

Tutti i dati trattati da tali categorie sono accessibili al solo personale debitamente formato e nominato con apposita lettera di nomina e vengono gestiti elettronicamente tramite il gestionale per la contabilità. A livello cartaceo sono riposti in archivi specifici divisi per categoria di interessato; quindi la Bolamì srl ha istruito il personale di riferimento sulla comunicazione immediata dei dati qualora ne venga fatta la richiesta da un interessato.

In tal senso viene consentito agli interessati di accedere ai propri dati per:

- Verificarne la veridicità;
- Modificarli nel caso divengano inesatti;
- Integrarli anche con dichiarazione integrativa;
- Richiederne la cancellazione;

**Accesso ai dati personali:** l'accesso ai dati personali è libero per gli autorizzati al trattamento dei dati, persone non autorizzate che dovranno accedere alla zona dell'archivio dovranno essere accompagnate per evitare l'accesso non consentito ai dati.

**Accesso ai dati sensibili o giudiziari:** l'accesso agli archivi contenenti dati sensibili o giudiziari è consentito esclusivamente a persone autorizzate. Non sono ammesse persone, anche se autorizzate, dopo l'orario di chiusura.

### ***Conservazione dei dati***

La Bolamì srl conserverà i dati degli interessati in una forma che consenta l'identificazione degli stessi per un arco temporale non superiore al conseguimento delle finalità per le quali sono stati raccolti.

I dati strettamente necessari per gli adempimenti fiscali, contabili e per la gestione del rapporto di lavoro, venuta meno la finalità per la quale erano stati raccolti, verranno comunque conservati per un periodo non superiore a 10 anni e comunque secondo disposizioni di cui all'art. 22 del DPR n. 600/1973.

### ***Cancellazione dei dati***

La Bolamì srl, in osservanza al corrispondente diritto di accesso all'interessato, ha predisposto procedure per le quali gli interessati possano richiedere la cancellazione senza ingiustificato ritardo dei dati personali o limitazione del trattamento dei dati personali che li riguardano, per i seguenti motivi:



- Perché i dati non sono più necessari per la finalità per i quali erano stati raccolti;
- Perché l'interessato ha revocato il consenso al trattamento dei dati,
- Perché l'interessato si oppone al trattamento;
- Perché i dati sono trattati illecitamente.

La Bolami srl ha previsto quindi che nei casi sopra citati il termine ultimo per la cancellazione sia di massimo 30 giorni.

## Misure di sicurezza idonee adottate a livello cartaceo

### Procedure di Custodia Atti e Documenti

- **Dati Comuni:** l'archivio degli atti e dei documenti contenente dati personali è consentito al solo personale autorizzato e debitamente formato, in un'area alla quale non è permesso l'accesso libero a persone non autorizzate al trattamento dei dati.
- **Accesso ai dati sensibili o giudiziari:** l'accesso agli archivi contenenti dati sensibili o giudiziari è consentito esclusivamente a persone autorizzate. Non sono ammesse persone, anche se autorizzate, dopo l'orario di chiusura.

Gli atti e i documenti sono conservati presso la nostra sede di cui sotto elenchiamo le caratteristiche.

Gli atti e i documenti, quando sono prelevati per essere utilizzati, dovranno essere rimessi al loro posto prima dell'orario di chiusura.

### Elenco delle sedi:

<b>Sede</b>	Sede legale
<b>Indirizzo</b>	Via Francesco Roncati, 9 - Bologna (BO)

### Elenco degli uffici

Ufficio	Sede legale		Sede		Sede legale
Incaricato alla custodia	Stefano Sarti		Incaricati presenti al lavoro in ufficio		1
Area videosorveglianza	SI	Sistema di allarme	NO	Accesso consentito al pubblico	NO
Armagli blindati	NO	Armagli ignifughi	NO	Armagli senza serratura	SI
Armagli con serratura	NO	Scaffalature	SI	Cassettiere senza serratura	NO

Cassette re con serratura	NO	Finestre c o n inferiate	NO	Finestre s e n z a inferiate	SI
Chiusura c o n serratura	SI	Chiusura s e n z a serratura	NO	Cassaforte	SI
Sistema antincendio	NO	E s i s t e registro accesso	NO	Estintori	2
Note					

## Misure di Sicurezza idonee adottate a livello elettronico

L'operatore potrà accedere ai computer ai quali è autorizzato esclusivamente inserendo le proprie credenziali e la propria password. L'addetto non potrà diminuire il livello di sicurezza stabilito dall'amministratore di sistema per il computer a cui accede. Per prevenire l'accesso ai dati da parte di operatori non autenticati, l'addetto che si dovrà allontanare dal proprio computer anche solo per pochi minuti, dovrà attivare CTRL+ALT+CANC con sblocco tramite il reinserimento della propria password di autenticazione.

L'addetto dovrà operare con diligenza ponendo estrema cura ed attenzione nell'utilizzo del computer e delle applicazioni al fine di evitare cancellazioni e modifiche errate, accidentali o intenzionali che possano arrecare danno o pregiudizio alla nostra organizzazione e per le quali sarà ritenuto responsabile.

L'addetto dovrà segnalare immediatamente al responsabile del trattamento dati eventuali anomalie di funzionamento dei computer, della rete del computer e delle applicazioni utilizzate.

Di seguito è riportato l'elenco degli strumenti elettronici utilizzati per il trattamento dei dati personali, alla data di redazione del presente documento.

PC	MAC MINI
Marca	APPLE
Sistema operativo	OSX
Modello	A1347
Antivirus	
Ufficio	Sede legale

PC	iPad Pro
Marca	APPLE
Sistema operativo	IOS
Modello	
Antivirus	

Ufficio	Sede legale
---------	-------------

### ***Sistema di Autenticazione***

Utilizzo di username e password. L'utente ricorda la propria username e la propria password che sono anche memorizzate sul sistema di accesso. Per un buon utilizzo della password sono state distribuite a tutti gli incaricati le Linee Guida per la corretta scelta della password.

### ***Sistema di Autorizzazione***

Autorizzazioni all'accesso ai dati secondo diversi livelli di responsabilità, limitate alle sole parti di trattamento per le quali sono stati assegnati compiti agli addetti, con limitazioni specifiche per ogni singolo addetto.

### ***Protezione da accessi non consentiti***

Nel caso di accessi non autorizzati verranno immediatamente bloccate tutte le operazioni su tutti i computer della rete e il responsabile della manutenzione dei computer disattiverà momentaneamente tutte le connessioni con internet. Verrà controllata tutta la rete dei computer, oltre a tutti i sistemi operativi, tutti i software installati e tutti i dati inseriti, per verificare eventuali danni provocati dagli accessi non autorizzati e per il ripristino della normalità.

Nel caso l'accesso non autorizzato sia stato effettuato per scopi fraudolenti o di sabotaggio, si provvederà all'immediata denuncia presso le forze di polizia e/o l'autorità giudiziaria dell'eventuale responsabile degli accessi non autorizzati.

Nel caso l'accesso non autorizzato sia stato effettuato con scopi non conformi alle norme interne della nostra organizzazione, ma comunque non a scopo fraudolento o di sabotaggio, verranno adottati tutti i provvedimenti previsti dalle leggi vigenti, dallo statuto dei lavoratori delle norme sindacali, dalle norme deontologiche.

Per prevenire l'accesso ai dati da parte di operatori non autenticati l'addetto attiva tramite CTRL+ALT+CANC il blocco del computer, consentendo lo sblocco solo ad operatori autorizzati.

### ***Protezione da trattamenti illeciti dei dati***

I dati sono protetti da un sistema di autenticazione che concede l'accesso agli addetti autenticati attraverso il riconoscimento di password d'accesso ai dati e che concede l'accesso agli addetti ai soli ambiti di trattamento dati a loro consentiti.

Nel caso di carenza di consapevolezza, disattenzione o incuria degli addetti, sarà bloccato temporaneamente l'accesso ai dati degli addetti e formato l'addetto sulle procedure del trattamento.

Nel caso di comportamenti sleali e fraudolenti degli addetti sarà bloccato immediatamente l'accesso ai dati degli addetti e adottati i relativi provvedimenti previsti dalle leggi vigenti, dallo statuto dei lavoratori, dalle norme sindacali, dalle norme deontologiche.

### ***Protezione da programmi informatici***

Su ogni PC e sul SERVER è attivo un software antivirus con frequenza automatica GIORNALIERA.

Sono state date istruzioni agli addetti su come prevenire, evitare e difendersi dai virus.

Nel caso di azione di virus informatici, verranno immediatamente bloccate tutte le operazioni su tutti i computer della rete attraverso l'utilizzo di un programma antivirus aggiornato e verrà immediatamente verificata e bonificata tutta la rete dei computer.

Nel caso di spamming, verranno immediatamente bloccate tutte le operazioni su tutti i computer della rete e il responsabile della manutenzione dei computer disattiverà momentaneamente tutte le connessioni con

Internet, verificherà i firmali su ogni computer e l'aggiornamento periodico dei programmi antivirus su ogni computer e tutta la rete dei computer.

Nel caso di azione dei programmi suscettibili di recare danno, verranno immediatamente bloccate tutte le operazioni su tutti i computer della rete e il responsabile della manutenzione dei computer disattiverà i programmi dannosi e verrà immediatamente verificata e bonificata tutta la rete dei computer.

### ***Procedure di backup***

Le copie di backup vengono effettuate:

- AUTOMATICAMENTE con frequenza GIORNALIERA su DISCO ESTERNO
- AUTOMATICAMENTE con frequenza GIORNALIERA su SERVER

### ***Procedure per la custodia delle copie di sicurezza***

Le copie di backup dei dati sono conservate presso:

- ufficio ARCHIVIO

Le copie settimanali dei backup vengono portate fuori dalla sede dal Responsabile dei Trattamenti e da lui custodite. Le copie di backup sono accessibili esclusivamente ad operatori autorizzati.

### **Le più importanti misure di sicurezza da adottare, in caso di utilizzo di strumenti informatizzati**

- Utilizzate sempre il codice identificativo personale e le parole chiave, cambiandole ogni qual volta abbiate la sensazione che esse non siano sufficientemente sicure; laddove possibile, utilizzate sempre almeno 8 caratteri, mescolando caratteri maiuscoli e minuscoli.
- La parola chiave deve essere preferibilmente priva di significato e non deve mai essere comunicata a soggetti terzi, anche se di fiducia.
- Ricordate che in caso di trattamento di dati sensibili, la parola chiave deve essere cambiata almeno ogni tre mesi, e se questo intervallo viene ridotto, tanto meglio.
- Si raccomanda di evitare di utilizzare la stessa parola chiave sia sui computer portatili che su quelli fissi.
- Accertatevi di effettuare con frequenza la copia di backup dei dati archiviati sul personal computer o supporto di memoria asportabile, sia trasferendoli sul floppy disk, sia trasferendoli su supporti informatizzati portatili. In questo caso, si faccia attenzione che le modalità di custodia di questi supporti portatili siano quelle applicate al computer principale.
- Non tenete mai insieme le copie di backup ed il personal computer, per evitare che un eventuale furto possa coinvolgere sia i dati del personal computer che quelli di backup.
- Tutte le precauzioni che vengono prese all'interno della azienda per filtrare virus e messaggi di posta elettronica non autorizzati, potrebbero non essere attive quando il personal computer viene collegato a una presa telefonica di un albergo. Si faccia quindi particolare attenzione, quando ci si collega ad Internet attraverso reti non dotate di appropriati filtri, al tipo di messaggio che viene ricevuto.
- Ci si accerti che il software antivirus presente sul personal computer sia costantemente aggiornato o che il sistema operativo ed altri applicativi residenti siano sempre aggiornati; accertarsi inoltre che il firewall, se presente, abbia un profilo di attività aggiornato.
- Quando ci si collega ad Internet, la prima operazione da fare è sempre quella di aggiornare il software antivirus, il software di base ed i software applicativi residenti; successivamente si può procedere con altre operazioni.

- Se scoprite che il vostro personal computer è infetto da virus, chiedete subito istruzioni al responsabile del trattamento sugli interventi da attuare, e non effettuate ulteriori elaborazioni.
- Collegatevi regolarmente al sito Internet del venditore degli applicativi residenti su personal computer, in modo da avere sempre a disposizione gli ultimi aggiornamenti, che molto spesso sono mirati non solo a migliorare la flessibilità d'uso dell'applicativo, ma anche e soprattutto la sua sicurezza.
- Non lasciate mai il personal computer collegato ad Internet senza il vostro presidio; anzi, cercate di tenervi collegati soltanto per il minimo tempo necessario per effettuare le operazioni desiderate.
- Non permettete ad alcuna persona, anche di fiducia, di accedere al vostro personal computer.

## **Istruzioni agli addetti al trattamento che trattano dati con strumenti elettronici corredate di Linee Guida per la Prevenzione dei Virus e per la scelta delle password**

Nell'ambito informatico, il termine "sicurezza" si riferisce a tre aspetti distinti:

1. **Riservatezza:** Prevenzione contro l'accesso non autorizzato alle informazioni
2. **Integrità:** Le informazioni non devono essere alterabili da incidenti o abusi
3. **Disponibilità:** Il sistema deve essere protetto da interruzioni impreviste

Il raggiungimento di questi obiettivi richiede non solo l'utilizzo di appropriati strumenti tecnologici, ma anche gli opportuni meccanismi organizzativi. Misure soltanto tecniche, per quanto possano essere sofisticate, non saranno efficienti se non usate propriamente. In particolare, le precauzioni di tipo tecnologico possono proteggere le informazioni durante il loro transito attraverso i sistemi, o anche quando queste rimangono inutilizzate su un disco di un computer; nel momento in cui esse raggiungono l'utente finale, la loro protezione dipende esclusivamente da quest'ultimo, e nessuno strumento tecnologico può sostituirsi al suo senso di responsabilità ed al rispetto delle norme.

- **Utilizzare le chiavi:** il primo livello di protezione di qualunque sistema è quello fisico: è vero che una porta chiusa può in molti casi non costituire una protezione sufficiente, ma è vero che pone se non altro un primo ostacolo, e richiede comunque uno sforzo volontario e non banale per la sua rimozione. È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e sbirciare i documenti posti su una scrivania; pertanto, chiudete a chiave il vostro ufficio e riponetevi i documenti negli appositi contenitori alla fine di ogni giornata di lavoro.
- **Conservare i documenti in luoghi sicuri:** tutti i documenti cartacei devono essere posti in contenitori con etichette che devono riportare un identificativo, ma mai con i nominativi di clienti, fornitori o contatti o qualsiasi altra informazione immediatamente riconducibile a persone fisiche. Tutti i contenitori con i documenti devono essere posti in scaffalature a giorno, se poste in luoghi controllati, o in armadi con serratura o ripostigli con porte con serratura se posti in luoghi non controllati o aperti al pubblico. I dati per cui viene richiesto il blocco o la cancellazione, ma che devono essere mantenuti per un obbligo di legge o a propria tutela in quanto relativi ad adempimenti contrattuali svolti, dovranno essere posti in armadi con serratura o ripostigli con porte con serratura. I dati sensibili o giudiziari dovranno sempre essere posti in armadi con serratura o ripostigli con porte con serratura, e sono consegnati agli incaricati sotto la loro responsabilità e, al di fuori dell'orario di lavoro, solo previa registrazione. I dati estremamente riservati dovranno essere posti in armadi blindati, casseforti o luoghi sicuri (locali in muratura con porta blindata). Non lasciare documenti con dati personali sui tavoli, dopo averli utilizzati, riponeteli sempre nei loro contenitori.
- **Conservare i CD in un luogo sicuro:** per i CD, DVD, dischetti, pen-drive e per qualsiasi altro supporto removibile di dati, si applicano gli stessi criteri che per i documenti cartacei, con l'ulteriore pericolo che il loro smarrimento (che può essere anche dovuto ad un furto) può passare più facilmente inosservato. Riponeteli quindi sotto chiave in armadi o archivi non appena avete finito di usarli.
- **Utilizzate le password:** vi sono svariate categorie di password, ognuna con il proprio ruolo preciso:

- la password di accesso al computer, che impedisce l'utilizzo improprio della vostra postazione quando per un motivo qualsiasi non vi trovate in ufficio;
- la password di accesso alla rete, che impedisce che l'eventuale accesso non autorizzato a una postazione renda disponibili tutte le risorse dell'ufficio;
- la password di programmi specifici, che impedisce l'accesso ai documenti realizzati con quelle applicazioni;
- la password del salvaschermo, infine, impedisce che una vostra assenza momentanea permetta ad una persona non autorizzata di visualizzare il vostro lavoro.

L'utilizzo di questi tipi fondamentali di password è obbligatorio. Imparatene l'utilizzo e, nel caso dobbiate comunicare anche se temporaneamente la vostra password ai tecnici incaricati dell'assistenza, registrate l'ora di comunicazione e di rinnovo della vostra password.

- **Attenzione alle stampe e ai fax di documenti riservati:** non lasciate accedere alle stampe o ai fax persone non autorizzate; se la stampante o il fax non si trovano sulla vostra scrivania, recatevi quanto prima a ritirare le stampe. Posizionate le stampanti e i fax in luoghi controllati e non accessibili al pubblico ed ai visitatori. Distruggete personalmente le stampe quando non servono più. È opportuno l'utilizzo di una macchina distruggi documenti, indispensabile nel caso di documenti sensibili o giudiziari.
- **Non utilizzate le mail per dati riservati:** non inviate MAI dati sensibili o riservati via email, come ad esempio numeri di carta di credito, password, numeri di conti bancari.
- **Prestate attenzione all'utilizzo dei computer portatili:** i computer portatili sono un facile bersaglio per i ladri. Se avete necessità di gestire dati riservati su un portatile, fatevi installare un buon programma di cifratura del disco rigido e utilizzate una procedura di backup periodico. Se durante la giornata vi spostate molto dalla vostra postazione o addirittura la notte lasciate il vostro portatile in ufficio, riponetelo in armadi chiusi a chiave.
- **Non fatevi spiare quando state digitando la password:** anche se molti programmi non ripetono in chiaro la password sullo schermo, quando digitate la vostra password questa potrebbe essere letta guardando i tasti che state battendo, anche se avete una buona capacità di digitazione.
- **Custodite la password in un luogo sicuro:** scrivete la vostra password, chiudetela in busta chiusa e consegnatela all'incaricato addetto alla sua custodia che provvederà a firmarla nei lembi di chiusura. Fate ben attenzione a non riscrivere la vostra password, l'unico affidabile dispositivo di registrazione è la vostra memoria.
- **Non fate usare il vostro computer a personale esterno a meno di non essere sicuri della loro identità e delle loro autorizzazioni:** personale esterno può avere bisogno di installare del nuovo software/hardware nel vostro computer: assicuratevi dell'identità della persona e delle autorizzazioni ad operare sul vostro computer.
- **Non utilizzate apparecchi non autorizzati:** l'utilizzo di modem su postazioni di lavoro collegati alla rete di edificio offre una porta d'accesso dall'esterno non solo al vostro computer, ma a tutti i dati dell'organizzazione. Per l'utilizzo consultatevi con il responsabile del trattamento dati.
- **Non installate programmi non autorizzati:** solo i programmi acquistati dalla vostra organizzazione con regolare licenza sono autorizzati. Se il vostro lavoro richiede l'utilizzo di programmi specifici consultatevi con il responsabile del trattamento dati.
- **Adottate con cura le linee guida per la prevenzione di virus:** la prevenzione dalle infezioni da virus sul vostro computer è molto più facile e comporta uno spreco di tempo minore della correzione degli effetti di un virus; tra l'altro, potreste incorrere in una perdita irreparabile di tutti i dati.
- **Controllate la politica locale relativa ai backup:** i vostri dati potrebbero essere gestiti su un server, oppure essere gestiti in locale e trasferiti in un server solo al momento del backup. Chiedete al responsabile del trattamento dati quali sono le operazioni di backup che dovete eseguire, con quali

modalità e con quali tempi. Il responsabile del trattamento curerà con estrema cura ed attenzione i backup periodici di tutti i dati.

- **Utilizzate gruppi di continuità:** verificate l'utilizzo di gruppi di continuità.
- **Segnalate le anomalie:** segnalate sempre, al più presto, al responsabile del trattamento dati qualsiasi tipo di anomalia si verifichi, sia nelle funzionalità del computer in cui operate, sia sulla rete di computer su cui operate, sia su qualsiasi altra applicazione che state utilizzando. Segnalare in tempo le anomalie e circostanziare gli eventi è fondamentale per prevenire problemi ben più consistenti.

## Linee guida per la prevenzione dei Virus

Un virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi. Alcuni virus si limitano a riprodursi senza ulteriori effetti, altri si limitano alla semplice visualizzazione di messaggi sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido.

### Come si trasmette un virus:

- attraverso programmi provenienti da fonti non ufficiali;
- attraverso le macro di alcuni programmi;
- attraverso le email ricevute;
- attraverso il download da Internet.

### Come NON si trasmette un virus:

- attraverso file di dati non in grado di contenere macro (file di testo, pdf, jpeg, ecc);
- attraverso email non contenenti allegati.

### Quando il rischio da virus si fa serio:

- quando si installano programmi;
- quando si copiano dati dai dischetti;
- quando si scaricano dati o programmi da internet.

### Quali effetti ha un virus?

- Effetti sonori e messaggi sconosciuti appaiono sul video.
- Nel menù appaiono funzioni extra finora non disponibili.
- Lo spazio sul disco si riduce inspiegabilmente.
- Le funzionalità dei computer rallentano repentinamente.

### Come prevenire i Virus

- **Usate soltanto programmi provenienti da fonti fidate:** copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato. Non utilizzare programmi non autorizzati dal responsabile del trattamento dei dati.

- **Assicuratevi di non far partire accidentalmente il vostro computer da dischetto, Cd o DVD:** infatti, se il dischetto fosse infettato, il virus si trasferirebbe nella memoria RAM e potrebbe espandersi ad altri file.
- **Assicuratevi che il vostro software antivirus sia aggiornato:** la tempestività nell'azione di bonifica è essenziale per limitare danni che un virus può causare; inoltre è vitale che il programma antivirus sia aggiornato periodicamente (non oltre sei mesi).
- **Assicuratevi che sul vostro computer sia attivato il Firewall:** verificate dalle preferenze del vostro computer o chiedete al responsabile del trattamento dati, che sul vostro computer sia attivato il Firewall e solo i privilegi di rete minimi necessari alle vostre esigenze d'accesso ai dati. Oltretutto, se sul vostro computer non vi collegate ad Internet o non inviate fax, staccate il cavo telefonico per evitare possibili accessi.
- **Non diffondete messaggi di provenienza dubbia:** se ricevete messaggi che avvisano di un nuovo virus pericolosissimo e che fanno riferimento ad una notizia proveniente dalla "Microsoft", ignoratelo. Le email di questo tipo sono dette con terminologia anglosassone hoax (termine spesso tradotto in italiano con "bufala").
- **Non partecipate a "catene di S. Antonio" e simili:** analogamente, tutti i messaggi che vi invitano a "diffondere la notizia quanto più possibile" sono hoax. Anche se parlano della fame nel mondo, della situazione delle donne negli stati arabi, di una bambina in fin di vita, se promettono guadagni miracolosi o grande fortuna, sono tutti hoax aventi spesso scopi molto simili a quelli dei virus, ossia utilizzare indebitamente le risorse informatiche.
- **Non aprite allegati alle email inviate da sconosciuti:** non aprite allegati alle email con file di tipo excel, zip, sit, doc contenente macro e qualsiasi altro formato a voi sconosciuto se non siete certissimi della provenienza. Potete aprire solamente allegati di tipo pdf, jpg e file di testo che non contengono macro.

## Scelta delle Password

Il più semplice metodo per l'accesso illecito ad un sistema consiste nell'indovinare la password dell'utente legittimo. In molti casi sono stati procurati seri danni al sistema informativo a causa di un accesso protetto da password "poco sicura". La scelta di password "sicure" è quindi parte essenziale della sicurezza informatica.

### Cosa NON fare

- **NON dite a nessuno la vostra password.** Ricordate che lo scopo principale per cui usate una password è assicurarvi che nessun altro possa utilizzare le vostre risorse o possa farlo a vostro nome.
- **NON scrivete la password da nessuna parte** che ne permetta facilmente la lettura, soprattutto vicino al computer.
- **NON scegliete password che si possano trovare su un dizionario.** Su alcuni sistemi è possibile provare tutte le password contenute in un dizionario per vedere quale sia quella giusta.
- **NON crediate che usare parole straniere renderà più difficile il lavoro di scoperta,** infatti chi vuole scoprire una password è dotato di molti dizionari delle più svariate lingue.
- **NON usate il Vostro nome utente.** È la password più semplice da indovinare.
- **NON usate password che possono in qualche modo essere legate a Voi** come ad esempio il vostro nome, quello di vostra moglie/marito, dei figli, del cane, date di nascita, numeri di, telefono, ecc.

### Cosa fare

- Cambiare la password a intervalli regolari. La normativa sulla privacy prevede che se sono trattati dati sensibili o giudiziari la password deve essere cambiata ogni tre mesi, altrimenti ogni sei mesi. La password deve essere lunga almeno otto caratteri, meglio se con un misto di lettere, numeri e segni di interpunzione.
- Utilizzate password differenti per l'accesso a differenti sistemi.
- Le migliori password sono quelle facili da ricordare ma allo stesso tempo difficili da indovinare, come quelle che si possono ottenere comprimendo frasi lunghe.



## Istruzioni agli addetti al trattamento che trattano dati senza l'utilizzo di strumenti elettronici

Di seguito si riportano le misure di sicurezza idonee da adottare a cura del Responsabile e degli addetti, in caso di trattamento di dati personali senza l'ausilio di strumenti elettronici.

Modalità tecniche da adottare a cura del titolare, del responsabile e dell'addetto, in caso di trattamento con strumenti diversi da quelli elettronici:

- agli addetti sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico - con cadenza almeno annuale - dell'individuazione dell'ambito del trattamento consentito ai singoli addetti, la lista degli addetti può essere redatta anche per classi omogenee di mansione e dei relativi profili di autorizzazione;
- quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli addetti del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate;
- quando gli atti e i documenti contenenti dati personali, sensibili o giudiziari sono affidati agli addetti del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli addetti fino alla restituzione, in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

Nell'ambito informatico il termine "sicurezza" si riferisce a tre aspetti distinti:

- **Riservatezza:** prevenzione contro l'accesso non autorizzato alle informazioni.
- **Integrità:** le informazioni non devono essere alterabili da incidenti o abusi.
- **Disponibilità:** il sistema deve essere protetto da interruzioni impreviste.

Il raggiungimento di questi obiettivi richiede non solo l'utilizzo di appropriati strumenti tecnologici, ma anche gli opportuni meccanismi organizzativi. Misure soltanto tecniche, per quanto possano essere sofisticate, non saranno efficienti se non usate propriamente. In particolare, le precauzioni di tipo tecnologico possono proteggere le informazioni durante il loro transito attraverso i sistemi, o anche quando queste rimangono inutilizzate su un disco di un computer. Nel momento in cui esse raggiungono l'utente finale, la loro protezione dipende esclusivamente da quest'ultimo, e nessuno strumento tecnologico può sostituirsi al suo senso di responsabilità ed al rispetto delle norme.

- **Utilizzare le chiavi:** il primo livello di protezione di qualunque sistema è quello fisico; è vero che una porta chiusa può in molti casi non costituire una protezione sufficiente, ma è vero che pone se non altro un primo ostacolo, e richiede comunque uno sforzo volontario e non banale per la sua rimozione. È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e sbirciare i documenti posti su una scrivania; pertanto, chiudete a chiave il vostro ufficio e riponete i documenti negli appositi contenitori alla fine di ogni giornata di lavoro.
- **Conservate i documenti in luoghi sicuri:** tutti i documenti cartacei devono essere posti in contenitori con etichette che devono riportare un identificativo, ma mai con i nominativi di clienti, fornitori o contatti o qualsiasi altra informazione immediatamente riconducibile a persone fisiche. Tutti i contenitori con i documenti devono essere posti in scaffalature a giorno, se poste in luoghi controllati, o armadi con serratura o ripostigli con porte con serratura, se posti in luoghi non controllati o aperti al pubblico. I dati per cui viene richiesto il blocco o la cancellazione, ma che devono essere mantenuti per un obbligo di legge o a propria tutela in quanto relativi ad adempimenti contrattuali svolti, dovranno essere posti in armadi con serratura o ripostigli con porte con serratura. I dati sensibili o giudiziari dovranno sempre essere posti in armadi con serratura o ripostigli con porte con serratura e sono consegnati agli incaricati sotto la loro responsabilità e, al di fuori dell'orario di lavoro, solo previa registrazione. I dati estremamente riservati dovranno essere posti in armadi blindati, casseforti o luoghi sicuri (locali in muratura con porta blindata). Non lasciare documenti con dati personali sui tavoli: dopo averli utilizzati, riponeteli sempre nei loro contenitori.

## Istruzioni agli addetti esterni del Trattamento

Gli addetti esterni del trattamento dei dati personali, devono scrupolosamente attenersi alle seguenti istruzioni che devono essere considerate ordine di servizio.

### **Principi generali da osservare**

Ogni trattamento di dati personali deve avvenire nel rispetto primario dei seguenti principi di ordine generale:

Ai sensi dell'art.5 del Reg. UE 679/16, che prescrive i "Principi applicabili al trattamento di dati personali" per ciascun trattamento di propria competenza, il Responsabile deve fare in modo che siano sempre rispettati i seguenti presupposti:

I dati devono essere trattati:

- secondo il principio di **liceità**, vale a dire conformemente alle disposizioni del Regolamento, nonché alle disposizioni del Codice Civile, per cui, più in particolare, il trattamento non deve essere contrario a norme imperative, all'ordine pubblico ed al buon costume;
- secondo il principio fondamentale di **correttezza**, il quale deve ispirare chiunque tratti qualcosa che appartiene alla sfera altrui;
- secondo il principio di **trasparenza**, che consente all'interessato di venire a conoscenza delle metodologie e delle finalità di utilizzo dei propri dati;
- secondo il principio di **adeguatezza**, il trattamento dei dati deve essere riferibile alla tipologia di incarico o mansione svolta;
- secondo il principio di **pertinenza**, ovvero i dati devono essere trattati in relazione allo scopo cui sono destinati;
- secondo il principio della **limitatezza**, la raccolta dei dati non può eccedere ai dati strettamente necessari per la finalità perseguita.

I dati devono essere raccolti solo per **scopi**:

- **esatti**, cioè precisi e rispondenti al vero e, se necessario, **aggiornati**;
- **conservati** per un periodo non superiore a quello necessario per gli scopi del trattamento e comunque in base alle disposizioni aventi ad oggetto le modalità ed i tempi di conservazione degli atti amministrativi. Trascorso detto periodo, i dati vanno resi anonimi o cancellati e la loro comunicazione e/o diffusione non è più consentita;
- trattati in modo tale che venga garantita un'adeguata sicurezza dei dati personali mediante misure tecniche ed organizzative adeguate;
- **determinati**, vale a dire che non è consentita la raccolta come attività fine a sé stessa;
- **espliciti**, nel senso che il soggetto interessato va informato sulle finalità del trattamento;
- **legittimi**, cioè, oltre al trattamento, come è evidente, anche il fine della raccolta dei dati deve essere lecito;

In particolare, i dati idonei a rivelare lo **stato di salute** o la **vita sessuale** sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo.

Ciascun trattamento deve, inoltre, avvenire nei limiti imposti dal principio fondamentale di **riservatezza** e nel rispetto della dignità della persona dell'interessato al trattamento, ovvero deve essere effettuato eliminando ogni occasione di impropria conoscibilità dei dati da parte di terzi.

Ciascun Addetto deve, inoltre, essere a conoscenza del fatto che, per la violazione delle disposizioni di cui al Regolamento Europeo in materia di trattamento dei dati personali, sono previste **sanzioni amministrative** e

**pecuniarie** (art. 83). Per le altre sanzioni riferibili alle violazioni non soggette a sanzioni amministrative e pecuniarie si rimanda alla legislazione nazionale.

In ogni caso, la responsabilità penale per eventuale uso non corretto dei dati oggetto di tutela resta a carico della singola persona cui l'uso illegittimo degli stessi sia imputabile.

In merito alla responsabilità civile si fa rinvio all'art.2050 del Codice Civile, che dispone relativamente ai danni cagionati per effetto del trattamento ed ai conseguenti obblighi di risarcimento, implicando a livello pratico che, per evitare ogni responsabilità, l'operatore è tenuto a fornire prova di avere applicato le misure tecniche di sicurezza più idonee a garantire appunto la sicurezza dei dati detenuti.

### **Compiti particolari dell'addetto esterno**

L'addetto esterno al trattamento dei dati personali, operando nell'ambito dei principi sopra ricordati, deve attenersi ai seguenti **compiti di carattere particolare**:

- identificare e censire i **trattamenti** di dati personali, le **banche dati** e gli **archivi** gestiti con supporti informatici e/o cartacei necessari all'espletamento delle attività istituzionalmente rientranti nella propria sfera di competenza;
- definire, per ciascun trattamento di dati personali, **la durata** del trattamento e la **cancellazione** o anonimizzazione dei dati obsoleti, nel rispetto della normativa vigente in materia di prescrizione e tenuta archivi;
- ogni qual volta si raccolgano dati personali, provvedere a che venga fornita **l'informativa** ai soggetti interessati, ai sensi degli artt.13 – 14 –21 del Regolamento;
- adempiere agli **obblighi di sicurezza**, quali attenersi alle disposizioni di cui agli artt. 25 e 32 del Regolamento, cioè adottare tutte le **preventive misure di Sicurezza** ritenute **idonee** al fine di ridurre al minimo il rischio di distruzione o perdita anche accidentale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- **comunicare** tempestivamente al Titolare casi di **accesso non autorizzato** ai dati o di trattamento non consentito o non conforme alle finalità perseguite;
- far osservare gli adempimenti previsti in caso di **nuovi trattamenti e cancellazione** di trattamenti;
- segnalare al Titolare l'eventuale cessazione di trattamento.

In merito agli addetti, l'addetto esterno deve:

- individuare tra i propri collaboratori, designandoli per iscritto, addetti al trattamento fornendo loro le **istruzioni** a cui devono attenersi per svolgere le operazioni di trattamento;
- **adoperarsi** al fine di rendere effettive le suddette istruzioni cui devono attenersi gli addetti del trattamento, curando in particolare il profilo della riservatezza, della sicurezza di accesso e della integrità dei dati e l'osservanza parte degli addetti, nel compimento delle operazioni di trattamento, dei principi di carattere generale che informano la vigente disciplina in materia;
- stabilire le modalità di **accesso** ai dati e l'organizzazione del lavoro degli addetti, avendo cura di adottare preventivamente le misure organizzative idonee e impartire le necessarie istruzioni ai fini di riscontro di eventuali richieste di esecuzione dei diritti di cui all'art.5, agli artt. 12 e ss. fino al 22 e all'art. 34;
- evadere le eventuali richieste di accesso, rettifica, integrazione, cancellazione, blocco dei dati da parte dell'interessato che eserciti i propri diritti ai sensi degli artt. di cui sopra;
- collaborare con il Titolare all'adempimento degli obblighi previsti dal Regolamento e segnalare eventuali problemi applicativi.

## Istruzioni del Responsabile del Trattamento

Il Responsabile del trattamento è debitamente nominato dal Titolare del trattamento in osservanza alle disposizioni dell'art.28.

Il responsabile del trattamento dei dati personali deve scrupolosamente attenersi alle seguenti istruzioni che devono essere considerate ordine di servizio.

### Principi generali da osservare

Ogni trattamento di dati personali deve avvenire nel rispetto primario dei seguenti principi di ordine generale. Ai sensi dell'art.5 del Reg. UE 679/16, che prescrive i "Principi applicabili al trattamento di dati personali" per ciascun trattamento di propria competenza, il Responsabile deve fare in modo che siano sempre rispettati i seguenti presupposti:

I dati devono essere trattati:

- secondo il principio di **liceità**, vale a dire conformemente alle disposizioni del Regolamento, nonché alle disposizioni del Codice Civile, per cui, più in particolare, il trattamento non deve essere contrario a norme imperative, all'ordine pubblico ed al buon costume;
- secondo il principio fondamentale di **correttezza**, il quale deve ispirare chiunque tratti qualcosa che appartiene alla sfera altrui;
- secondo il principio di **trasparenza**, che consente all'interessato di venire a conoscenza delle metodologie e delle finalità di utilizzo dei propri dati;
- secondo il principio di **adeguatezza**, il trattamento dei dati deve essere riferibile alla tipologia di incarico o mansione svolta;
- secondo il principio di **pertinenza**, ovvero i dati devono essere trattati in relazione allo scopo cui sono destinati;
- secondo il principio della **limitatezza**, la raccolta dei dati non può eccedere ai dati strettamente necessari per la finalità perseguita.

I dati devono essere raccolti solo per **scopi**:

- **esatti**, cioè precisi e rispondenti al vero e, se necessario, **aggiornati**
- **conservati** per un periodo non superiore a quello necessario per gli scopi del trattamento e comunque in base alle disposizioni aventi ad oggetto le modalità ed i tempi di conservazione degli atti amministrativi. Trascorso detto periodo, i dati vanno resi anonimi o cancellati e la loro comunicazione e/o diffusione non è più consentita;
- trattati in modo tale che venga garantita un'adeguata sicurezza dei dati personali mediante misure tecniche ed organizzative adeguate;
- **determinati**, vale a dire che non è consentita la raccolta come attività fine a sé stessa;
- **espliciti**, nel senso che il soggetto interessato va informato sulle finalità del trattamento;
- **legittimi**, cioè, oltre al trattamento, come è evidente, anche il fine della raccolta dei dati deve essere lecito;

In particolare, i dati idonei a rivelare lo **stato di salute** o la **vita sessuale** sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo.

Ciascun trattamento deve, inoltre, avvenire nei limiti imposti dal principio fondamentale di **riservatezza** e nel rispetto della dignità della persona dell'interessato al trattamento, ovvero deve essere effettuato eliminando ogni occasione di impropria conoscibilità dei dati da parte di terzi.

Ciascun addetto deve, inoltre, essere a conoscenza del fatto che, per la violazione delle disposizioni di cui al Regolamento Europeo in materia di trattamento dei dati personali, sono previste **sanzioni amministrative e pecuniarie** (art. 83). Per le altre sanzioni riferibili alle violazioni non soggette a sanzioni amministrative e pecuniarie si rimanda alla legislazione nazionale.

In ogni caso, **la responsabilità penale** per eventuale uso non corretto dei dati oggetto di tutela, resta a carico della singola persona cui l'uso illegittimo degli stessi sia imputabile.

In merito **alla responsabilità civile** si fa rinvio all'art. 2050 del Codice Civile, che dispone relativamente ai danni cagionati per effetto del trattamento ed ai conseguenti obblighi di risarcimento, implicando a livello pratico che, per evitare ogni responsabilità, l'operatore è tenuto a fornire prova di avere applicato le misure tecniche di sicurezza più idonee a garantire appunto la sicurezza dei dati detenuti.

### **Compiti particolari dell'addetto esterno**

L'addetto esterno al trattamento dei dati personali, operando nell'ambito dei principi sopra ricordati, deve attenersi ai seguenti **compiti di carattere particolare**:

- identificare e censire i **trattamenti** di dati personali, le **banche dati** e gli **archivi** gestiti con supporti informatici e/o cartacei necessari all'espletamento delle attività istituzionalmente rientranti nella propria sfera di competenza;
- definire, per ciascun trattamento di dati personali, **la durata** del trattamento e la **cancellazione** o anonimizzazione dei dati obsoleti, nel rispetto della normativa vigente in materia di prescrizione e tenuta archivi;
- ogni qual volta si raccolgano dati personali, provvedere a che venga fornita **l'informativa** ai soggetti interessati, ai sensi degli artt. 13 – 14 – 21 del Regolamento;
- adempiere agli **obblighi di sicurezza**, quali attenersi alle disposizioni di cui agli artt. 25 e 32 del Regolamento, cioè adottare tutte le **preventive misure di Sicurezza** ritenute **idonee** al fine di ridurre al minimo il rischio di distruzione o perdita anche accidentale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- **comunicare** tempestivamente al Titolare casi di **accesso non autorizzato** ai dati o di trattamento non consentito o non conforme alle finalità perseguite;
- far osservare gli adempimenti previsti in caso di **nuovi trattamenti e cancellazione** di trattamenti;
- segnalare al Titolare l'eventuale cessazione di trattamento.

In merito agli addetti, l'addetto esterno deve:

- individuare tra i propri collaboratori, designandoli per iscritto, addetti al trattamento fornendo loro le **istruzioni** cui devono attenersi per svolgere le operazioni di trattamento;
- **adoperarsi** al fine di rendere effettive le suddette istruzioni cui devono attenersi gli addetti del trattamento, curando in particolare il profilo della riservatezza, della sicurezza di accesso e della integrità dei dati e l'osservanza parte degli addetti, nel compimento delle operazioni di trattamento, dei principi di carattere generale disposti dalla vigente disciplina in materia;
- stabilire le modalità di **accesso** ai dati e l'organizzazione del lavoro degli addetti, avendo cura di adottare preventivamente le misure organizzative idonee e impartire le necessarie istruzioni ai fini di riscontro di eventuali richieste di esecuzione dei diritti di cui all'art.5, agli artt. 12 e ss. fino al 22 e all'art. 34;
- evadere le eventuali richieste di accesso, rettifica, integrazione, cancellazione, blocco dei dati da parte dell'interessato che eserciti i propri diritti ai sensi degli artt. di cui sopra;
- collaborare con il Titolare all'adempimento degli obblighi previsti dal Regolamento e segnalare eventuali problemi applicativi.

## **Piano Formativo**

In questa sezione sono riportate le informazioni necessarie per individuare il quadro sintetico degli interventi formativi che si prevede di svolgere.

Descrizione sintetica degli interventi formativi	Classi di incarico o tipologie di incaricati interessati	Tempi previsti
Formazione sulla protezione dei dati	Francesca Pungetti	1 anno

In osservanza alle disposizioni dell'art. 28 e art. 32 comma 4 del Reg. EU 679/16, tutti i soggetti addetti al trattamento dei dati personali devono essere in grado di fornire al Titolare garanzie professionali sufficienti che soddisfino i requisiti di formazione e competenza richiesti dalla natura dell'incarico. A tal proposito, gli interventi formativi rivolti agli addetti dei trattamenti hanno la finalità di rendere loro edotti:

1. sulla segretezza della componente riservata della credenziale e sulla diligente custodia dei dispositivi in possesso ed uso esclusivo dell'addetto;
2. sulla custodia e l'accessibilità dello strumento elettronico durante una sessione di trattamento;
3. sul controllo e sulla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali;
4. sul controllo e sulla custodia degli atti e i documenti contenenti dati personali sensibili o giudiziari a loro affidati per lo svolgimento dei relativi compiti, fino alla restituzione al termine delle operazioni in maniera che ad essi non accedano persone prive di autorizzazione;
5. sulle procedure aziendali da applicare per la sicurezza e la protezione dei dati, quali ad esempio il cambio delle password, il salvataggio dei dati, aggiornamenti di antivirus e tutto quanto necessario a far sì che le misure di sicurezza reputate idonee dall'azienda vengano a tutti gli effetti messe in pratica;
6. sui profili di autorizzazione e gli ambiti di applicazione degli stessi riferiti per classi omogenee di addetti;
7. sulle policy aziendali in riferimento all'utilizzo della posta elettronica ed internet, sul sistema di videosorveglianza e sull'Amministratore di sistema qualora la struttura ne necessiti;
8. sui diritti dell'interessato ex artt. dal 15 al 22.

Il piano formativo del personale viene inoltre redatto tenendo conto dei seguenti criteri:

- a) aggiornamento sistematico delle istruzioni agli addetti;
- b) verifica costante delle istruzioni impartite agli addetti;
- c) aggiornamento periodico sulle misure di sicurezza adottate.

## PROGETTO PIANO FORMATIVO

La struttura aziendale ha solo un profilo di autorizzazione, quindi basterà svolgere un unico intervento formativo di circa 2 ore con tutto il personale addetto, per far sì che tutta l'azienda sia responsabilizzata sulle procedure aziendali e sul quadro normativo di riferimento.

A tal proposito di seguito si trova il progetto formativo

Addetti da formare	Modalità di formazione	Tempi di attuazione	Verifica di attuazione
Francesca Pungetti	corso on line		

Addetti da formare	Modalità di formazione	Tempi di attuazione	Verifica di attuazione
Stefano Sarti	corso on line		

## Dichiarazione di avvenuta formazione

Di seguito è riportata la dichiarazione per attestare l'avvenuta formazione fornita da ai responsabili e agli addetti al trattamento.

Incaricato/Responsabile	Data formazione	Firma
Francesca Pungetti	09/03/2023	

Incaricato/Responsabile	Data formazione	Firma
Stefano Sarti	09/03/2023	

Con la firma si dà atto di aver ricevuto da parte di idonea formazione finalizzata al corretto trattamento dei dati personali, ed in particolare di essere edotto:

- sulla segretezza della componente riservata della credenziale e sulla diligente custodia dei dispositivi in possesso ed uso esclusivo dell'addetto;
- sulla custodia e l'accessibilità dello strumento elettronico durante una sessione di trattamento;
- sul controllo e sulla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali;
- sul controllo e sulla custodia degli atti e i documenti contenenti dati personali sensibili o giudiziari a loro affidati per lo svolgimento dei relativi compiti, fino alla restituzione al termine delle operazioni in maniera che ad essi non accedano persone prive di autorizzazione;
- sulle procedure aziendali da applicare per la sicurezza e la protezione dei dati, quali ad esempio cambio delle password, il salvataggio dei dati, aggiornamenti di antivirus e tutto quanto necessario a far sì che le misure di sicurezza reputate idonee dall'azienda vengano a tutti gli effetti messe in pratica;
- sui profili di autorizzazione e gli ambiti di applicazione degli stessi riferiti per classi omogenee di addetti;
- sulle policy aziendali in riferimento all'utilizzo della posta elettronica ed internet, sul sistema di videosorveglianza e sull'Amministratore di sistema qualora la struttura ne necessiti;
- sui diritti dell'interessato ex artt. dal 15 al 22.

## Valutazione dei Rischi

Illustrazione dettagliata delle risultanze e piano di azione raccomandato

### 1. Obiettivi della valutazione dei rischi

L'attività di audit sulla valutazione dei rischi si è concentrata sui seguenti aspetti:

### 1.1 - Gestione della protezione dei dati

L'attività di audit ha verificato fino a che punto sono attuati i principi di responsabilità nella protezione dei dati, le politiche e le procedure, i controlli in grado di misurare il livello di prestazione della protezione, i meccanismi di individuazione e segnalazione della congruità con i vigenti regolamenti in materia di protezione dei dati personali. Questa attività è stata svolta in tutti i dipartimenti dell'organizzazione.

### 1.2 – Addestramento e sensibilizzazione

L'attività di audit ha verificato le modalità con cui è stata impartita e tenuta sotto controllo la formazione dei soggetti coinvolti nella protezione e trattamento dei dati personali, nonché la dettagliata conoscenza dei requisiti in materia di protezione dei dati personali, in relazione ai ruoli ed alle responsabilità dei singoli soggetti coinvolti. In particolare, l'auditor ha verificato se tutti i soggetti coinvolti abbiano sottoscritto uno specifico obbligo di riservatezza sul trattamento dei dati loro affidati, o se esiste altro obbligo formalizzato di riservatezza.

### 1.3 – Gestione manuale ed elettronica dei dati personali

L'attività di audit ha verificato i processi attuati dall'organizzazione per la gestione di supporti, sia manuali (cartacei) sia elettronici, che contengono dati personali. L'attività di audit ha verificato inoltre i controlli applicati, in grado di monitorare la creazione, la manutenzione, l'archiviazione, il trasporto, la comunicazione e la diffusione, la conservazione e la distruzione di supporti contenenti dati personali.

### 1.4 – Sicurezza dei dati personali

L'attività di audit ha verificato le misure tecniche ed organizzative attuate, in grado di garantire un adeguato livello di sicurezza sui dati personali, custoditi su supporti cartacei od elettronici.

### 1.5 – Congruità dell'informativa

Come più volte sottolineato nel Regolamento europeo sulla protezione dei dati, un'informativa accurata, intelligibile e corretta rappresenta un aspetto essenziale in qualsiasi forma di acquisizione e trattamento di dati. In fase di audit abbiamo esaminato tutte le varie informative che vengono fornite dal titolare del trattamento, preferibilmente conformi ai modelli proposti dal Parlamento europeo o ad altri modelli che potranno essere predisposti dalla Commissione europea, cercando di esaminarli dal punto di vista di un interessato non particolarmente competente e preparato nel settore.

### 1.6 – Correttezza delle procedure di raccolta del consenso

La raccolta del consenso rappresenta il naturale completamento dell'offerta di informativa. Si ripete, a questo proposito, la necessità che il consenso sia espresso in forma "granulare", in modo che siano da evitare consensi generalizzati, afferenti a molteplicità di utilizzo dei dati personali raccolti. Anche in questo caso, l'auditor ha esaminato il modulo di raccolta del consenso mettendosi nei panni di un interessato non particolarmente competente preparato nel settore.

### 1.7 – Determinazione del tempo di conservazione del dato

Come regola generale, un dato deve essere conservato per il tempo minimo necessario per raggiungere le finalità per le quali il dato è stato raccolto. In fase di raccolta del dato è pertanto indispensabile attribuire ad esso se non un periodo minimo di conservazione, almeno un criterio sulla base del quale possa essere successivamente determinata la data ultima di conservazione. Attenzione deve anche essere prestata alle modalità grazie le quali i dati, al termine del periodo utile di trattamento, vengono eliminati. Esistono procedure normative europee applicabili sia alla cancellazione di dati su supporto cartaceo, sia su altri supporti.



## 1.8 – Attività di comunicazione e diffusione di dati personali

L'attività di audit ha verificato se le procedure applicate, relative alla comunicazione e diffusione di dati personali, siano pienamente rispettose dei vigenti regolamenti e congrue con le indicazioni date dal responsabile e dall'incaricato del trattamento dei dati personali. In questo ambito, verranno in particolare analizzate le modalità di gestione di siti internet ed intranet, indipendentemente dal fatto che questi siti abbiano o meno la possibilità di raccogliere dati personali in fase di consultazione.

## 1.9 – Attività di trattamento svolta in paesi terzi

L'attività di audit ha verificato se le procedure applicate, relative all'eventuale trattamento di dati in paesi terzi, siano pienamente rispettose dei vigenti regolamenti e congrue con le indicazioni date dal responsabile e dall'incaricato del trattamento dei dati personali.

## 2. I livelli della valutazione

Le osservazioni e le raccomandazioni che seguono nel paragrafo successivo sono classificate secondo un livello di importanza, che viene definito in questa tabella.

L'Auditor auspica che il responsabile e l'incaricato del trattamento prendano buona nota di questi livelli di valutazione, in modo da pianificare appropriatamente le eventuali attività correttive e migliorative.

Codice colore	Opinione dell'Auditor	Livello di priorità della raccomandazione	Definizione
<b>Verde</b>	Elevato livello di congruità	V e n g o n o evidenziati solo aspetti di modesta rilevanza	Vi è un elevato livello di fiducia sul fatto che i processi e le procedure in atto garantiscano un adeguato livello di protezione dei dati. L'audit ha individuato solo alcune aree di modesta rilevanza per interventi di miglioramento alla situazione esistente e pertanto non si ritiene che siano necessari ulteriori significativi interventi per ridurre il rischio di non conformità con i dettati del regolamento.
<b>Giallo</b>	Accettabile livello di congruità	Gli aspetti esaminati sono a bassa priorità	Vi è un ragionevole livello di fiducia sul fatto che i processi e le procedure in atto garantiscano un adeguato livello di protezione dei dati. L'audit ha individuato alcune aree ove è opportuno effettuare interventi di miglioramento alla situazione esistente, al fine di ridurre il rischio di non conformità con i dettati del regolamento.

<b>Arancio</b>	Scarso livello di congruità	Gli aspetti esaminati sono a media priorità	Vi è un modesto livello di fiducia sul fatto che i processi e le procedure in atto garantiscano un adeguato livello di protezione dei dati. L'audit ha individuato varie aree bisognose di interventi di miglioramento alla situazione esistente, onde ridurre il rischio di non conformità con i dettati del regolamento.
<b>Rosso</b>	Insoddisfacente Livello di congruità	Gli aspetti esaminati sono ad alta priorità	Vi è un basso livello di fiducia sul fatto che i processi e le procedure in atto garantiscano un adeguato livello di Protezione dei dati. L'audit ha individuato rischi significativi di mancato rispetto dei dettati di regolamento in varie aree.

### 3. Illustrazione dettagliata delle risultanze e piano di azione raccomandato

Gestione della protezione dei dati		
CODICE E TITOLO	RISULTATO	RACCOMANDAZIONI
Risultanza A1 Organigramma aziendale	A livello strutturale e di lettere di nomina l'azienda non è conforme	Provvedere a conformare al Reg. UE 679/2016
Risultanza A2 Procedure tecniche ed organizzative di verifica e controllo	L'azienda ha previsto che le procedure vengano verificate direttamente da Titolare del trattamento	Nessuna raccomandazione

Addestramento e sensibilizzazione		
CODICE E TITOLO	RISULTATO	RACCOMANDAZIONI
Risultanza B1 Svolgimento di corsi di formazione sulla privacy	Sono stati effettuati corsi di formazione sulla privacy	Nessuna raccomandazione
Risultanza B3 Predisposizione di un piano formativo	è stato predisposto un piano formativo	Nessuna raccomandazione

<b>Gestione manuale ed elettronica dei dati personali</b>		
<b>CODICE E TITOLO</b>	<b>RISULTATO</b>	<b>RACCOMANDAZIONI</b>
Risultanza C1 Definizione di chi può trattare i dati	I documenti aventi dati personali vengono trattati solo da personale nominato e formato	Nessuna raccomandazione
Risultanza C2 Presenza di registri di accesso a dati sensibili e giudiziari	Non si trattano dati sensibili e giudiziari	Nessuna raccomandazione
Risultanza C3 Distruzione dei documenti contenenti dati personali	Tutti i documenti da cestinare contenenti dati personali vengono distrutti con trituratore	Nessuna raccomandazione
Risultanza C4 Separazione dei dati sensibili e giudiziari	I dati sensibili e giudiziari non vengono conservati separatamente dagli altri documenti e riposti in archivi chiusi a chiave	provvedere alla custodia per la conservazione dei dati sensibili o giudiziari in maniera secretata
Risultanza C5 Sicurezza dello strumento elettronico incustodito	A dispositivo incustodito si attiva il salvaschermo che sloggia l'utente	Nessuna raccomandazione

<b>Sicurezza dei dati personali</b>		
<b>CODICE E TITOLO</b>	<b>RISULTATO</b>	<b>RACCOMANDAZIONI</b>
Risultanza D1 Autenticazione informatica	E' stata predisposta l'autenticazione informatica per ogni utente	Nessuna raccomandazione
Risultanza D3 Istruzioni sulle modalità di conservazione, composizione e aggiornamento della parola chiave	All'interno delle lettere di nomina predisposte anche negli anni precedenti sono specificate istruzioni sulle modalità di conservazione, composizione e aggiornamento della parola chiave	Nessuna raccomandazione
Risultanza D6 Antivirus	Nessun o non tutti i PC sono dotati di antivirus che viene aggiornato annualmente dal titolare	predisporre immediatamente un antivirus per i dispositivi elettronici

Risultanza D7 Aggiornamento dei programmi	I programmi vengono aggiornati costantemente dal titolare	Nessuna raccomandazione
Risultanza D14 Piano di Emergenza	Il Piano di Emergenza è stato predisposto	Nessuna raccomandazione

<b>Congruità della informativa</b>		
------------------------------------	--	--

CODICE E TITOLO	RISULTATO	RACCOMANDAZIONI
Risultanza E1 Procedura di consegna dell'informativa	Ad ogni nuovo cliente non viene fatta firmare l'informativa	consegnare e far firmare ad ogni interessato l'informativa

<b>Correttezza delle procedure di raccolta del consenso</b>		
---	--	--

CODICE E TITOLO	RISULTATO	RACCOMANDAZIONI
Risultanza F1 Procedure per raccolta del consenso granulare	Il consenso è attualmente predisposto come da normativa europea	Conformare alla normativa europea
Risultanza F2 Procedure per la gestione dei consensi	E' stata predisposta la procedura di gestione dei consensi richiesti	Nessuna raccomandazione

<b>Procedure di Classificazione del livello di protezione dei dati</b>		
--	--	--

CODICE E TITOLO	RISULTATO	RACCOMANDAZIONI
Risultanza G1 Procedure di classificazione del livello di protezione dei dati	Sono predisposte procedure di classificazione di tipologie di dato	Nessuna raccomandazione

<b>Determinazione del tempo di conservazione del dato</b>		
<b>CODICE E TITOLO</b>	<b>RISULTATO</b>	<b>RACCOMANDAZIONI</b>
Risultanza H1 Determinazione del tempo di conservazione del dato	Non è stato determinato un tempo per la conservazione dei dati personali	individuare il tempo di conservazione per le diverse tipologie di dati

#### **Misure di sicurezza adottate**

#### **4. Sintesi delle risultanze dell'audit**

##### Aree esaminate

1. Gestione della protezione dei dati;
2. Addestramento e sensibilizzazione;
3. Gestione manuale ed elettronica dei dati personali;
4. Sicurezza dei dati personali;
5. Congruità dell'informativa;
6. Correttezza delle procedure di raccolta del consenso;
7. Determinazione del tempo di conservazione del dato;
8. Attività di comunicazione e diffusione di dati personali;
9. Attività di trattamento svolta in paesi terzi.

Interventi migliorativi raccomandati:

#### **RACCOMANDAZIONI TECNOLOGICHE**

- provvedere a disattivare le credenziali in disuso
- predisporre immediatamente un antivirus per i dispositivi elettronici
- Valutare la possibilità di diversificare l'uso di USB consentendolo solo a soggetti autorizzati

## RACCOMANDAZIONI ORGANIZZATIVE

- provvedere alla custodia per la conservazione dei dati sensibili o giudiziari in maniera secretata
- consegnare e far firmare ad ogni interessato l'informativa
- procedere a classificare i dati per tipologia di dati
- individuare il tempo di conservazione per le diverse tipologie di dati
- provvedere ad una nomina formale entro Maggio 2018

### 5. Opinione dell'Auditor

L'obiettivo dell'audit è quello di offrire al responsabile ed all'incaricato del trattamento una valutazione oggettiva ed indipendente del livello con cui l'attività svolta dall'organizzazione, in materia di trattamento di dati, è congrua con vigenti regolamenti e disposizioni.

Per facilitare la lettura dell'opinione dell'Auditor, i commenti sono inseriti nella tabella seguente e classificati in funzione del livello di assicurazione di congruità maturato dall'Auditor stesso.

Livello congruità	Commenti dell'auditor
-------------------	-----------------------

## MOLTO BASSO

Il livello di assicurazione di congruità, come valutato dall'Auditor, porta a ritenere che il rispetto dei regolamenti e disposizioni in materia di dati personali, a livello di processi e procedure, sia basso. L'audit ha identificato molte aree dove è possibile effettuare interventi di miglioramento, per raggiungere un accettabile livello di congruità con le esigenze di protezione dei dati.

Nello specifico:

- provvedere alla custodia per la conservazione dei dati sensibili o giudiziari in maniera secretata
- predisporre consegna brevimano o tramite invio di posta elettronica del disciplinare
- provvedere a disattivare le credenziali in disuso
- predisporre immediatamente un antivirus per i dispositivi elettronici
- Valutare la possibilità di diversificare l'uso di USB consentendolo solo a soggetti autorizzati
- consegnare e far firmare ad ogni interessato l'informativa
- procedere a classificare i dati per tipologia di dati
- individuare il tempo di conservazione per le diverse tipologie di dati
- provvedere alla richiesta di autorizzazione prima dell'istallazione delle videocamere
- provvedere ad una nomina formale entro Maggio 2018

Un piano dettagliato dei possibili interventi migliorativi, afferenti alle carenze individuate, viene presentato successivamente nella sezione dedicata alla illustrazione dettagliata dell'audit e di un piano di azione.

<b>BASSO</b>	<p>Il livello di assicurazione di congruità, come valutato dall'Auditor, porta a ritenere che il rispetto dei regolamenti e disposizioni in materia di dati personali, a livello di processi e procedure, sia basso. L'audit ha identificato molte aree dove è possibile effettuare interventi di miglioramento, per raggiungere un accettabile livello di congruità con le esigenze di protezione dei dati.</p> <p>Nello specifico:</p>
<b>ACCETTABILE</b>	<p>Il livello di assicurazione di congruità, come valutato dall'Auditor, porta a ritenere che il rispetto dei regolamenti e disposizioni in materia di dati personali, a livello di processi e procedure, sia accettabile. L'audit ha identificato molte aree dove è possibile effettuare interventi di miglioramento, per raggiungere un accettabile livello di congruità con le esigenze di protezione dei dati.</p> <p>Nello specifico:</p>



## SODDISFACENTE

Il livello di assicurazione di congruità, come valutato dall'Auditor, porta a ritenere che il rispetto dei regolamenti e disposizioni in materia di dati personali, a livello di processi e procedure, sia soddisfacente. L'audit ha identificato molte aree dove è possibile effettuare interventi di miglioramento, per raggiungere un accettabile livello di congruità con le esigenze di protezione dei dati.

Nello specifico:

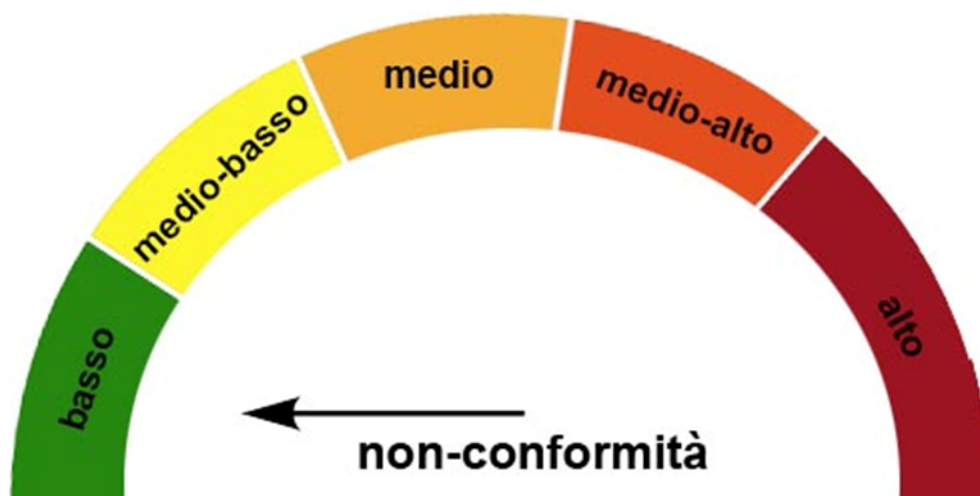
- L'azienda ha previsto che le procedure vengano verificate direttamente da Titolare del trattamento
- Sono stati effettuati corsi di formazione sulla privacy
- è stato predisposto un piano formativo
- I documenti aventi dati personali vengono trattati solo da personale nominato e formato
- Non si trattano dati sensibili e giudiziari o sono stati previsti registri di accesso al trattamento di dati sensibili e giudiziari al di fuori dell'orario lavorativo
- Tutti i documenti da cestinare contenenti dati personali vengono distrutti con tritacarte
- A dispositivo incustodito si attiva il salvaschermo che slogga l'utente
- E' stata predisposta l'autenticazione informatica per ogni utente
- All'interno delle lettere di nomina predisposte anche negli anni precedenti sono specificate istruzioni sulle modalità di conservazione, composizione e aggiornamento della parola chiave
- I programmi vengono aggiornati costantemente dal titolare
- Recupero dei dati tramite copie di backup
- Il consenso è attualmente predisposto come da normativa italiana
- Sono predisposte procedure di classificazione di tipologie di dato

## Conclusioni dell'Audit

In virtù delle risultanze precedentemente definite e specificate, si evince che, come da grafico successivo, in base alla valutazione dei rischi la struttura ha attualmente un rischio medio, in quanto le carenze e le inosservanze riferibili alle violazioni contrassegnate in rosso ed arancione nel grafico di cui sopra sono da considerare più rilevanti e potenzialmente dannose rispetto alle inosservanze rilevate in verde e giallo nel suddetto grafico.

Ne deriva, secondo una media ponderabile, un rischio medio tendente all'alto.

## Livello di non conformità

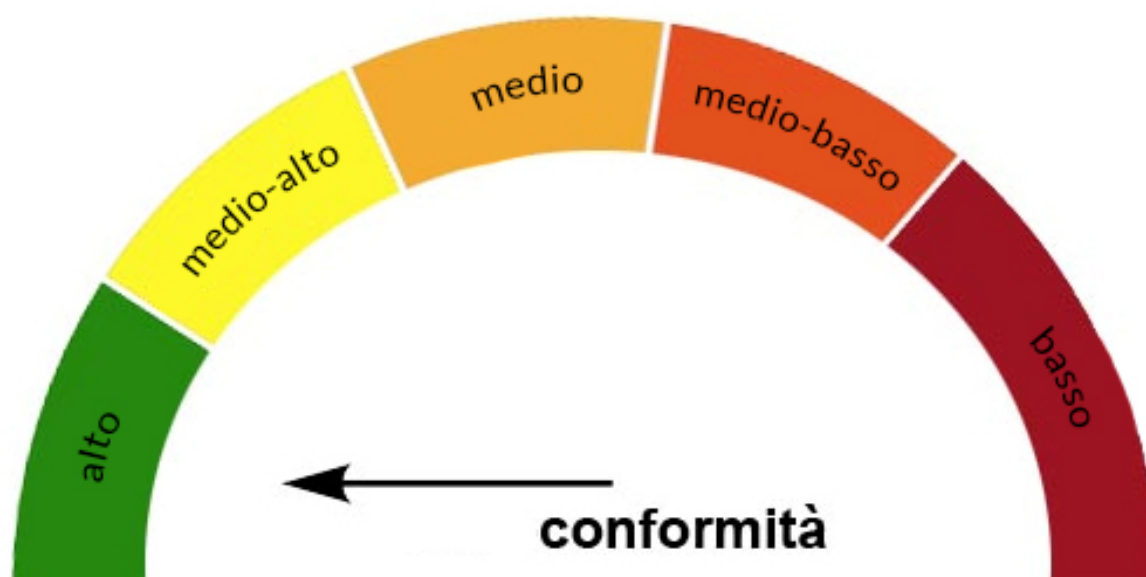


## Riepilogo di conformità

Osservando le raccomandazioni di seguito riportate e avendo proceduto alla generazione dei documenti così come previsti dalla normativa vigente, la situazione di conformità finale dello studio/azienda è così evidenziata:

- provvedere alla custodia per la conservazione dei dati sensibili o giudiziari in maniera secretata
- predisporre consegna brevimano o tramite invio di posta elettronica del disciplinare
- provvedere a disattivare le credenziali in disuso

- predisporre immediatamente un antivirus per i dispositivi elettronici
- Valutare la possibilità di diversificare l'uso di USB consentendolo solo a soggetti autorizzati
- consegnare e far firmare ad ogni interessato l'informativa
- procedere a classificare i dati per tipologia di dati
- individuare il tempo di conservazione per le diverse tipologie di dati
- provvedere alla richiesta di autorizzazione prima dell'installazione delle videocamere
- provvedere ad una nomina formale entro Maggio 2018



## 6. Tabella dei tempi di attuazione delle raccomandazioni

Raccomandazione	Stato di attuazione a 3 mesi	Stato di attuazione a 6 mesi
provvedere alla custodia per la conservazione dei dati sensibili o giudiziari in maniera secretata		

Raccomandazione	Stato di attuazione a 3 mesi	Stato di attuazione a 6 mesi
predisporre consegna brevimano o tramite invio di posta elettronica del disciplinare		

Raccomandazione	Stato di attuazione a 3 mesi	Stato di attuazione a 6 mesi
provvedere a disattivare le credenziali in disuso		

Raccomandazione	Stato di attuazione a 3 mesi	Stato di attuazione a 6 mesi
predisporre immediatamente un antivirus per i dispositivi elettronici		

Raccomandazione	Stato di attuazione a 3 mesi	Stato di attuazione a 6 mesi
Valutare la possibilità di diversificare l'uso di USB consentendolo solo a soggetti autorizzati		

Raccomandazione	Stato di attuazione a 3 mesi	Stato di attuazione a 6 mesi
consegnare e far firmare ad ogni interessato l'informativa		

Raccomandazione	Stato di attuazione a 3 mesi	Stato di attuazione a 6 mesi
procedere a classificare i dati per tipologia di dati		

Raccomandazione	Stato di attuazione a 3 mesi	Stato di attuazione a 6 mesi
individuare il tempo di conservazione per le diverse tipologie di dati		

Raccomandazione	Stato di attuazione a 3 mesi	Stato di attuazione a 6 mesi
provvedere alla richiesta di autorizzazione prima dell'installazione delle videocamere		

Raccomandazione	Stato di attuazione a 3 mesi	Stato di attuazione a 6 mesi
provvedere ad una nomina formale entro Maggio 2018		

## Piano di Emergenza

Nell'ottica dell'importanza della circolazione dei dati e della necessità di gestirne il flusso e il lecito trattamento, bisogna provvedere ad attuare azioni correttive in seguito al verificarsi di eventi dannosi o pericolosi per il trattamento dei dati personali.

In relazione alle misure di sicurezza predisposte, la Bolami srl ha messo a punto un quadro delle possibili intromissioni o effrazioni ai sistemi informatici (attacco di un virus, hackeraggio, furto dati, programmatore che sbaglia una query ed estrae tutti i dati personali) alle quali ha associato le relative azioni correttive.

1. Nel caso di accessi non autorizzati, verranno immediatamente bloccate tutte le operazioni su tutti i computer della rete e il responsabile della manutenzione dei computer disattiverà momentaneamente tutte le connessioni con Internet. Verrà controllata tutta la rete dei computer, oltre a tutti i sistemi operativi, tutti i software installati e tutti i dati inseriti per verificare eventuali danni provocati dagli accessi non autorizzati e per il ripristino della normalità.
2. Nel caso l'accesso non autorizzato sia stato effettuato per scopi fraudolenti, o di sabotaggio, si provvederà all'immediata denuncia presso le forze di polizia e/o l'autorità giudiziaria dell'eventuale responsabile degli accessi non autorizzati.
3. Nel caso l'accesso non autorizzato sia stato effettuato con scopi non conformi alle norme interne della nostra organizzazione, ma comunque non a scopo fraudolento o di sabotaggio, verranno adottati tutti i provvedimenti previsti dalle leggi vigenti, dallo statuto dei lavoratori, dalle norme sindacali, dalle norme deontologiche.

In ogni caso, per ognuna delle situazioni sopra citate o comunque per tutte le violazioni dei dati si provvederà a dare tempestiva comunicazione all'autorità garante come procedura prevista nel modulo in allegato.

Per accesso non autorizzato si intende:

- l'accesso effettuato da un operatore non autenticato utilizzando le credenziali di autenticazione di un addetto;
- l'accesso effettuato aggirando il sistema di autenticazione;
- l'accesso effettuato da un addetto autenticato in aree non previste dal sistema di autorizzazioni;
- l'accesso tramite intercettazioni di informazioni in rete;
- l'accesso non autorizzato a locali/aree ad accesso non riservato;
- l'accesso a strumenti contenenti dati che sono stati sottratti.

4. Nel caso di comportamenti sleali e fraudolenti degli addetti, sarà bloccato immediatamente l'accesso ai dati degli addetti e adottati i relativi provvedimenti previsti dalle leggi vigenti, dallo statuto dei lavoratori, dalle norme sindacali, dalle norme deontologiche.
5. Nel caso di azione di virus informatici, verranno immediatamente bloccate tutte le operazioni su tutti i computer della rete attraverso l'utilizzo di un programma antivirus aggiornato e verrà immediatamente verificata e bonificata tutta la rete dei computer.
6. Nel caso di spamming, verranno immediatamente bloccate tutte le operazioni su tutti i computer della rete e il responsabile della manutenzione dei computer disattiverà momentaneamente tutte le connessioni con Internet, verificherà i firewall su ogni computer e l'aggiornamento periodico dei programmi antivirus su ogni computer e tutta la rete dei computer.
7. Nel caso di azione dei programmi suscettibili di recare danno, verranno immediatamente bloccate tutte le operazioni su tutti i computer della rete e il responsabile della manutenzione dei computer disattiverà i programmi dannosi e verrà immediatamente verificata e bonificata tutta la rete dei computer.

Valutando le criticità emerse dalla valutazione dei rischi si può considerare il livello di rischio della Bolamì srl come MEDIO-BASSO constatandosi un elevato livello di fiducia sul fatto che i processi e le procedure in atto garantiscano un adeguato livello di protezione dei dati.

Il Piano di emergenza elaborato dalla Bolamì srl di cui sopra si riferisce a quelle azioni fortemente negative elencate precedentemente.

In relazione a quegli eventi dannosi che comportano un elevato livello di criticità per il dato personale stesso, la Bolamì srl ha previsto un tempo di ripristino pari a 7 giorni per i seguenti casi di violazioni illecite o accidentali di dati:

- Perdita
- Distruzione
- Modifica
- Divulgazione non autorizzata
- Accesso ai dati personali che siano trasmessi, conservati o trattati

Al fine di ripristinare gli archivi e dati, si è provveduto a conservare in un luogo esterno alla sede copie aggiornate settimanalmente sia dei dati che dei software (applicativi e sistemi operativi).

In aggiunta a ciò, il fornitore della Bolamì srl garantisce la consegna di strumenti elettronici con la stessa configurazione entro tre giorni dall'avvenuta violazione, considerando il tempo minimo di un giorno per l'installazione del sistema operativo e dei software applicativi.

Il trattamento di tutti i dati processati sarà ripristinato entro i 7 giorni del termine di cui sopra.

Nella definizione del piano di emergenza, la Bolamì srl ha predisposto eventi formativi per tutti gli addetti e i responsabili del trattamento dati nell'ottica di definire le azioni consentite e quelle non consentite agli stessi soggetti interessati. Nello stesso ambito, ha fornito dovuta e comprovata formazione dei possibili eventi negativi e delle relative azioni correttive da attuare, in modo tale da rendere note agli addetti ed ai responsabili del trattamento le procedure da attivare per risolvere o contenere l'effetto negativo scaturito dall'evento dannoso.

### **Responsabili o consulenti e autorità da contattare in caso di emergenza**

Il Titolare del Trattamento a norma dell'art. 33 del Regolamento, qualora la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, è tenuto ad effettuare senza ingiustificato ritardo, entro massimo le 72 ore dal momento in cui ne è venuto a conoscenza, la notificazione presso l'autorità competente, di cui all'art.55, della avvenuta violazione.

Nel caso di violazione che comporti un rischio consistente per i diritti e le libertà delle persone fisiche, la comunicazione va fatta all'autorità competente e contestualmente all'interessato come dispone l'art.34.

La Bolami srl si fa carico di adottare tutte le misure idonee a prevenire o risolvere eventuali eventi dannosi e di comunicare tempestivamente ogni violazione avvenuta presso l'autorità competente a norma dell'art. 83.