GESTIONE PRIVACY
ITEM SRL TESSUTI SRL
Ai sensi del D.lgs. n. 101 del 10/08/2018
e del Regolamento (UE)2016/679

1. PANORAMICA DEL TRATTAMENTO

Il presente documento definisce l'attuazione, all'interno di ITEM S.R.L. del disposto normativo D.lgs 101/2018 per l'adeguamento della normativa nazionale alle disposizioni del 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 norme relative alla libera circolazione di tali dati.

Con il presente documento si provvede:

a) alla identificazione e investitura dei soggetti responsabili.

b) alla identificazione dei soggetti destinatari della tutela.

c) alla descrizione del sistema informatico in uso.

d) alla classificazione e identificazione dei dati trattati.

e) alla valutazione dei rischi che possono influenzare la disponibilità, l'integrità e la confidenzialità dei dati.

f) alla individuazione dei criteri tecnici ed organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi.

g) alla individuazione dei criteri e delle procedure necessarie al fine di assicurare l'integrità dei dati.

h) alla individuazione dei criteri e delle procedure necessarie per la sicurezza delle trasmissioni dei dati.

i) alla definizione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati.

j) alla definizione di un piano periodico di revisione.

Ambito di applicazione

Il presente documento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di ITEM S.R.L.. indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.

DEFINIZIONI

Si riporta di seguito le responsabilità dei soggetti coinvolti.

1) «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;

2) «trattamento»: 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;

3) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4) «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

5) «pseudonimizzazione»:il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

6) «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

7) «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;

8) «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;

9) «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;

10) «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

11) «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

12) «violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

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

14) «dati biometrici»: i 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;

15) «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;

16) «stabilimento principale»:

a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;

b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

17) «rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

18) «impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

19) «gruppo imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

20) «norme vincolanti d'impresa»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

21) «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

22) «autorità di controllo interessata»: un'autorità di controllo interessata dal trattamento di dati personali in quanto:

a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;

b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure c) un reclamo è stato proposto a tale autorità di controllo;

23) «trattamento transfrontaliero»:

a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro;

oppure b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

24) «obiezione pertinente e motivata»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

25) «servizio della società dell'informazione»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio;

26) «organizzazione internazionale»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati

STANDARD APPLICABILI AL TRATTAMENTO

In dettaglio verranno riportati:
- i dati personali in questione, i loro destinatari e i periodi di conservazione.
- descrizione dei processi e delle risorse dedicate alla gestione dei dati personali per l'intero ciclo di vita dei dati stessi (dalla raccolta alla cancellazione).

Sono trattati tutti i dati riguardanti il trattamento ossia qualsiasi operazione compiuta con

l’ausilio, di processi automatizzati e applicate a dati personali, come raccolta, registrazione, l'organizzazione, la strutturazione, la conservazione l'adattamento, o la modifica, l'estrazione, la consultazione.
Per quanto riguarda la Classificazione dei dati trattati e modalità di trattamento, sono definiti tre livelli di dati:

Livello 1 - Dati Personali

Si tratta di 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;

Livello 2 – Dati Identificativi

Si tratta di dati personali che permettono l’identificazione diretta dell’interessato, come i dati anagrafici (nome, cognome), le immagini etc.

Livello 3 – Dati Sensibili e Giudiziari

I Dati sensibili: sono quei dati che possono 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, lo stato di salute e la vita sessuale;

I Dati giudiziari: quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato.

Con l'evoluzione delle nuove tecnologie, altri dati personali hanno assunto un ruolo significativo, come quelli relativi alle **comunicazioni elettroniche** (via Internet o telefono) e quelli che consentono la **geolocalizzazione**, fornendo informazioni sui luoghi frequentati e sugli spostamenti.

I dati personali *sono*:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

Il titolare del trattamento è competente per il rispetto del precedente paragrafo e in grado di comprovarlo («responsabilizzazione»).

QUAL È IL CICLO DI VITA DEL TRATTAMENTO DEI DATI

Di seguito viene riportato il ciclo di vita dei dati (dalla raccolta alla distruzione passano per la loro conservazione di vari step del trattamento, l'archiviazione, etc.), servendosi di un diagramma di flusso dei dati (in allegato) e fornendo una dettagliata descrizione di ciascun processo effettuato. Le risorse su cui si basano i trattamenti dei dati personali che possono comprendere hardware, software, reti, persone, supporti cartacei o documentazione.

Il ciclo di vita dei dati personali

Il D.lgs 101/2008 e il nuovo Regolamento Europeo introducono tra le righe il concetto di privacy by design e privacy by default. Questo approccio pone al centro di tutto, il ciclo di vita dell'informazione: quali dati è davvero necessario raccogliere, in che modo, e cosa è possibile farci.

La protezione dei dati by design considera un approccio che consente di mettere in moto un processo logico che permetterà di proteggere i dati in maniera efficiente.

Privacy per impostazione predefinita significa che una volta che un prodotto o un servizio è stato rilasciato al pubblico, le impostazioni sulla privacy più severe dovrebbero essere applicate per impostazione predefinita, senza alcun input manuale da parte dell'utente finale. Inoltre, i dati personali forniti dall'utente per consentire l'uso ottimale di un prodotto devono essere conservati solo per il tempo necessario a fornire il prodotto o il servizio. Se vengono divulgate più informazioni del necessario per fornire il servizio, la "privacy per impostazione predefinita".

La raccolta del dato

Archiviazione e protezione

Un passaggio fondamentale per ogni organizzazione è quello di definire dove e per quanto tempo conservare i dati raccolti. Deve essere definito un periodo di conservazione per ciascun tipo di dato

motivandolo in rapporto alle esigenze del trattamento e/o all'esistenza di vincoli di legge. Occorre distinguere tra dati correnti e dati archiviati, il cui accesso sarà limitato ai soli soggetti interessati. È necessario implementare un meccanismo di soppressione per archiviare i dati correnti o eliminare i dati archiviati al termine del loro periodo di conservazione. Inoltre è necessario eliminare le tracce funzionali e i log tecnici che non possono essere conservati a tempo indeterminato.

L' acquisizione di un dato passa attraverso il consenso dell'interessato che deve conoscere che utilizzo verrà fatto con quella informazione.

Accesso e utilizzo

A ciascun dipendente sarà assegnato un processo di responsabilità in base alla loro possibilità di accedere ai dati e di utilizzarli (amministrazione, marketing, vendite, customer service, risorse umane etc.).

Tutte informazioni sono contenute **nel registro dei trattamenti**.

La cancellazione dei dati

La cancellazione dei dati è un diritto fondamentale previsto dalla normativa vigente .

LICEITÀ DEL TRATTAMENTO

Ogni trattamento deve trovare fondamento in un'idonea base giuridica; i fondamenti di liceità del trattamento sono indicati dal Dlgs. 101/2018 e dal regolamento 2016/679.
Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:
a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

MINIMIZZAZIONE DEI DATI

Si tratta di ridurre la gravità dei rischi limitando la raccolta di dati personali al minimo necessario per la specifica finalità. Evitare di raccogliere dati non necessari, di utilizzare dati che non abbiano alcun rapporto con la specifica finalità e di produrre impatti eccessivi sulle persone.
Il **principio di minimizzazione** dei dati fa parte dei principi in base ai quali si effettua il trattamento dei dati. Salvo poche eccezioni, un titolare deve trattare solo i dati di cui ha realmente bisogno per raggiungere le finalità del trattamento.
Il principio di 'minimizzazione' si declina nei seguenti profili:

- **Adeguatezza** dei dati, vale a dire proporzionalità rispetto alle finalità per la quale sono raccolti .
- **Pertinenza** dei dati rispetto alle finalità precedentemente definite.
- **Limitazione** dei trattamenti solo per il raggiungimento delle finalità.

Dunque i dati raccolti devono essere adeguati e pertinenti rispetto al fine che si intende perseguire, ed essi non possono essere raccolti in misura maggiore a quella necessaria.
A questo proposito è da introdurre un altro principio, ovvero quello **dell'esattezza dei dati**.
I dati trattati devono essere esatti e, se necessario, aggiornati. Il titolare deve, in questo senso, prendere tutte le misure ragionevoli per cancellare o rettificare tempestivamente quelli che non sono più esatti.

MISURE A TUTELA DEI DIRITTI DEGLI INTERESSATI

Consenso degli interessati

La richiesta del consenso deve essere presentata in modo distinto da altre richieste, e seppur non è necessaria la forma scritta, la richiesta deve avvenire in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro.
Quando per un trattamento è necessario il consenso, il titolare deve essere in grado di dimostrare che il consenso è stato effettivamente prestato.
Il titolare è tenuto ad agevolare l'esercizio dei diritti da parte dell'interessato e, in particolare, a fornire un riscontro alla richiesta del medesimo senza ingiustificato ritardo e comunque entro un mese dal ricevimento della medesima (Capo III, art.12).
Il Titolare deve esplicitare il periodo di conservazione dei dati personali, ovvero i criteri utilizzati per determinare tale periodo; il linguaggio dell'informativa deve essere semplice e chiaro (Capo III, artt.13 – 14).
Gli interessati devono dare un consenso libero, specifico e informato con la quale manifestano il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

Diritto di accesso

L'interessato ha diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati personali e altre informazioni.
Disposizioni particolari si applicano all'accesso ai dati sanitari, in base al diritto nazionale, e anche all'esercizio del diritto di accesso da parte dei titolari della potestà genitoriale, per i minori, ovvero da parte del rappresentante legale, per i soggetti sottoposti a misure di tutela.

Diritto alla portabilità dei dati

Gli interessati hanno il diritto di ricevere in un formato strutturato, di uso comune e leggibile da un dispositivo automatico i dati personali che li riguardano forniti a un titolare del trattamento, e hanno

il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui i dati personali sono stati comunicati.

Il "Codice in materia di protezione dei dati personali (link isexternal)" prevede all'art. 7 che chiunque possa conoscere se i propri dati personali sono trattati da una qualsiasi azienda, PA, ente, associazione, o altro (cioè da un qualsiasi titolare di trattamento). Se il titolare effettivamente tratta i suoi dati personali, l'interessato, cioè la persona cui tali dati si riferiscono, ha il diritto di:

- sapere come i propri dati sono stati ottenuti dal titolare, chi all'interno dell'organizzazione del titolare tratta in pratica tali dati, quali sono le finalità dei trattamenti effettuati;
- ottenere la rettifica dei propri dati personali se questi non sono aggiornati o completi;
- opporsi al trattamento dei propri dati personali (se ciò non è in contrasto con eventuali altri obblighi contrattuali o di legge); l'opposizione è sempre valida se le finalità del trattamento sono l'invio di materiale pubblicitario o di vendita diretta o ricerche di mercato o comunicazione commerciale.

Diritti di rettifica e di cancellazione (diritto all'oblio)

Il diritto all'oblio consente a un individuo, autore di un reato in passato, di richiedere che il fatto non sia più pubblicizzato o divulgato dalla stampa e da altri mezzi di informazione (Internet incluso). Questo, però, a patto che dall'evento sia trascorso molto tempo e non sia tornato a essere di pubblico interesse e di pubblico dominio. Insomma, grazie al diritto all'oblio chiunque può chiedere la non divulgazione (o la rimozione) di notizie ritenute lesive della propria reputazione dopo un congruo lasso di tempo.

L 'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

- a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
- b) l'interessato revoca il consenso su cui si basa il trattamento conformemente,se non sussiste altro fondamento giuridico per il trattamento;

- c) l’interessato si oppone al trattamento, non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell’articolo 21, paragrafo 2;
- d) i dati personali sono stati trattati illecitamente;
- e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell’Unione o dello Stato membro cui è soggetto il titolare del trattamento;
- f) i dati personali sono stati raccolti relativamente all’offerta di servizi della società dell’informazione.
- 2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell’interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.
- 3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:
- a) per l’esercizio del diritto alla libertà di espressione e di informazione;
- b) per l’adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell’Unione o dello Stato membro cui è soggetto il titolare del trattamento;
- c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell’articolo 9, paragrafo 2, lettere h) e i), e dell’articolo 9, paragrafo 3;
- d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all’articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o
- e) per l’accertamento, l’esercizio o la difesa di un diritto in sede giudiziaria

Diritti di limitazione

1. L ’interessato ha il diritto di ottenere dal titolare del trattamento **la limitazione** del trattamento quando ricorre una delle seguenti ipotesi:

a) l’interessato contesta l’esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l’esattezza di tali dati personali;

b) il trattamento è illecito e l’interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l’utilizzo;

c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.
2. Se il trattamento è limitato a norma del paragrafo 1, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.
3. L 'interessato che ha ottenuto la limitazione del trattamento a norma del paragrafo 1 è informato dal titolare del trattamento prima che detta limitazione sia revocata.

Diritto di opposizione

L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano .

RESPONSABILITÀ CONNESSE AL TRATTAMENTO ITEM S.R.L..

Il Titolare del trattamento è ITEM S.R.L.., il Responsabile del trattamento è l'Amministratore Angelo Ciccone, nel rispetto delle disposizioni in materia di trattamento dei dati personali, nonché di garantire la tutela dei diritti dell'interessato.

Titolare del trattamento

L'amministratore ha la responsabilità finale e assume le decisioni fondamentali afferenti al trattamento dei dati personali.

ALLEGATO_ Visura camerale CCIAA azienda ITEM S.R.L..

Responsabili del trattamento

Il responsabile del trattamento (nel nuovo regolamento europeo data processor) è la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento (art. 4, par. 1, n. 8).
Si tratta di un soggetto che deve essere in grado di fornire garanzie al fine di assicurare il pieno rispetto delle disposizioni in materia di trattamento dei dati personali, nonché di garantire la tutela dei diritti dell'interessato.

ALLEGATO_	Identificazione Responsabile/ Incaricati al trattamento
ALLEGATO_	Incarico e accettazione del Responsabili del trattamento

Amministratore di sistema

Nella specifica realtà la funzione di Amministratore di Sistema è stata affidata al Titolare del trattamento ITEM S.R.L...

ALLEGATO_	Incarico e accettazione dell'Amministratore del Sistema
ALLEGATO_	Condizioni generali di utilizzo del Sistema Informativo

Tale figura ricopre anche l'incarico di preposto custode delle parole chiave.

ALLEGATO_	Incarico e accettazione del Custode parole chiave

Incaricati del trattamento

Il titolare del trattamento ha rilevato all'interno della realtà ITEM S.R.L. la necessità di formalizzare gli incarichi al trattamento, ognuno nell'ambito della propria area di competenza, come riportato nel registro del trattamento.

Figure particolari

Medico competente

Il medico competente, è trattato dall'azienda come "titolare del trattamento", in questo caso il consenso informato relativo alla sorveglianza sanitaria ai sensi del D.Lgs. 81/08 non compete all'azienda ma al Medico Competente.

Prestatori di servizi

La ITEM S.R.L.. ha deciso di predisporre specifica richiesta di garanzie ai prestatori di servizi (ad esempio: Società di elaborazione paghe, software house …), in quanto questi si trovano a trattare dati personali di cui è titolare ITEM S.R.L...

Prestatore di Servizi devono assicurare l'adozione presso la propria organizzazione delle misure di sicurezza obbligatorie informatiche ed organizzative.

ALLEGATO_ Garanzie dati terzi

Soggetti interessati

Con riferimento ai "Soggetti cui i dati si riferiscono" il Titolare del trattamento ha individuato le seguenti necessità:

ALLEGATO_ Informativa ai Dipendenti

ALLEGATO_ Informativa ai Visitatori

ALLEGATO_ Informativa ai Clienti e Fornitori

ALLEGATO_ Clausola da inserire nei contratti

ALLEGATO_	Consenso informato per curricula
ALLEGATO_	Cupon per e-mail commerciali
ALLEGATO_	La Privacy Policy del sito
ALLEGATO_	Garanzie dati terzi

Il Sistema informativo ITEM S.R.L..

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer, espone la ITEM S.R.L.. ai rischi di un coinvolgimento sia patrimoniale sia penale, creando problemi alla sicurezza e all'immagine dell'Azienda stessa.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche della nostra Azienda deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro. ITEM S.R.L.. ha adottato un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.

Utilizzo del Personal Computer

Il Personal Computer affidato al dipendente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. La stessa password deve essere attivata per l'accesso alla rete. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del Titolare del trattamento.

Il custode delle parole chiave riservate, per l'espletamento delle sue funzioni, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica interna ed esterna.

Il custode delle parole chiave riservate potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere alla stessa azienda, titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate dalla stessa azienda, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività aziendale nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio in caso di prolungata assenza od impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato.

Non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione esplicita del Titolare, in quanto sussiste il grave pericolo di portare Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal Titolare della ITEM S.R.L... L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'azienda a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (D. Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.

Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo previa autorizzazione esplicita del Titolare.

Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. In ogni caso deve essere attivato lo screen saver e la relativa password.

Non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ed altre periferiche), se non con l'autorizzazione espressa del Titolare.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il Titolare nel caso in cui vengano rilevati virus.

Utilizzo della rete della ITEM S.R.L.

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup.

Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.

Il Titolare del trattamento può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.

Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.

È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. È buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

Classificazione dei dati trattati e modalità di trattamento

Sono definiti tre livelli di dati:

Livello 1 – Dati Personali

Livello 2 – Dati Identificativi

Livello 3 – Dati Sensibili e Giudiziari

Per ognuno di questi livelli vengono previste le misure di sicurezza per quanto riguarda il trattamento dei dati personali effettuato con strumenti elettronici e non.

Trattamento con strumenti elettronici

Di seguito sono riportate le modalità di trattamento da adottare a cura di, ITEM S.R.L. dei Responsabili al trattamento e dagli incaricati, in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la

relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

Sistema di autorizzazione

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.
13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Altre misure di sicurezza

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del

codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.
18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

19. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all' art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.
20. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.
21. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
22. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

Misure di tutela e garanzia

23. Il titolare che adotta misure di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.

Trattamenti senza l'ausilio di strumenti elettronici

Di seguito sono riportate le modalità tecniche da adottare a cura di dei Responsabili del trattamento e degli incaricati, in caso di trattamento con strumenti diversi da quelli elettronici:

24. Agli incaricati 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 incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
25. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati 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.
26. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli

archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

IDENTIFICAZIONE DEI DATI TRATTATI

Vengono di seguito identificati e classificati i dati particolari trattati da ITEM S.R.L.. elencando le modalità di trattamento (automatico o manuale), il responsabile del trattamento ed i sistemi (informatici e non) coinvolti nella specifica realtà aziendale.

Lista tipologie dei dati

ID	CATEGORIA	DESCRIZIONE	SPECIFICHE TIPOLOGIA

	COMUNI	Nominativo Indirizzo o altri elementi di identificazione personale	nome, cognome, età, sesso, cittadinanza o nazionalità, indirizzo privato, indirizzo di lavoro, numero telefono, posizione rispetto agli obblighi militari, n. carta di identità, passaporto, patente di guida, posizione pensionistica, codice fiscale, targa automobilistica, dati fisici (altezza, peso, etc.)
ID	**CATEGORIA**	**DESCRIZIONE**	**SPECIFICHE TIPOLOGIA**
	COMUNI	Dati relativi alla famiglia e a situazioni personali	Stato civile, figli, soggetti a carico, consanguinei, altri appartenenti al nucleo familiare.

3	**COMUNI**	Lavoro	Occupazione attuale e precedente, informazioni su reclutamento, informazioni sulla cessazione dall'impiego, curriculum lavorativo, retribuzioni e trattenute, beni aziendali in possesso del dipendente, benefits e altro, dati sulla gestione e sulla valutazione delle attività lavorative, formazione, cariche pubbliche rivestite.
ID	**CATEGORIA**	**DESCRIZIONE**	**SPECIFICHE TIPOLOGIA**
4	**COMUNI**	Attività economiche, commerciali, finanziarie e assicurative	Dati contabili, ordini, buoni di spedizione, fatture, articoli, prodotti, servizi etc., contratti, accordi, transazioni finanziarie, identificativi finanziari, redditi, investimenti, passività, solvibilità, prestiti/mutui, ipoteche, crediti, indennità, benefici, concessioni, donazioni sussidi, contributi, dati assicurativi, dati previdenziali

5	**COMUNI**	Istruzione e Cultura	Curriculum di studi e accademico, pubblicazioni, articoli, monografie, relazioni, materiale audiovisivo
ID	**CATEGORIA**	**DESCRIZIONE**	**SPECIFICHE TIPOLOGIA**
6	**COMUNI**	Beni proprietà possessi	Proprietà, possessi e locazioni beni e servizi forniti o ottenuti
7	**SENSIBILI**	Informazioni concernenti taluni procedimenti giudiziari, stato di salute	Dati relativi a procedimenti diversi dai provvedimenti di cui all'art. 3 comma1, lettere da a) a o) e da r) a u), del dpr. 14 novembre 2002, n.313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale. Dati sulla salute

•

Modalità di trattamento

Tutti i dati sopra elencati riportano nelle colonne dedicate identificazione della modalità di trattamento che può essere cartacea o informatica.

Viene inoltre specificata la posizione cartacea e il supporto informativo Computer.

Responsabilità

La responsabilità nel trattamento dei dati viene definita per ogni tipologia nella tabella sopra riportata.

Tutti gli incaricati sono stati preventivamente autorizzati e hanno ricevuto specifica informazione sulle procedure di sicurezza da implementare nella gestione dei dati.

ANALISI DEI RISCHI

Vengono illustrati i potenziali rischi a cui potrebbero essere soggetti i siti e i sistemi di trattamento dei dati sulla base dell'esperienza e della conoscenza dell'ambiente di lavoro.

I rischi sono classificati in base all'impatto che possono avere sulle tre caratteristiche di disponibilità, integrità e discrezionalità dei dati.

Disponibilità dei dati

- Guasti hardware
- Incendio
- Alluvione
- Rottura di condutture dell'acqua
- Malfunzionamento software
- Errore nella configurazione del sistema hardware/software
- Interruzione dell'alimentazione elettrica
- Sovratensioni sull'alimentazione elettrica
- Furto dell'hardware
- Interruzione della connettività WAN
- Interruzione della connettività LAN
- Infezione da virus

•

- Attacco di tipo Denial of service (DoS malfunzionamento dovuto ad un attacco informatico in cui si fanno esaurire deliberatamente le risorse di un sistema informatico che fornisce un servizio ai client, ad esempio un sito web su un web server, fino a renderlo non più in grado di erogare il servizio ai client richiedenti)

Integrità dei dati

- Rottura hardware
- Malfunzionamento software
- Cancellazione o modifica accidentale
- Cancellazione o modifica fraudolenta
- Infezione da virus

Discrezionalità dei dati

- Furto dell'hardware
- Furto dei dati in formato elettronico da parte di personale esterno
- Furto dei dati in formato elettronico da parte di personale interno
- Furto dei dati in formato cartaceo da parte di personale esterno
- Furto dei dati in formato cartaceo da parte di personale interno
- Accesso accidentale ai dati in formato elettronico
- Accesso accidentale ai dati in formato cartaceo
- Accesso non autorizzato ai dati da rete interna
- Accesso non autorizzato ai dati da rete esterna
- Accesso con cavalli di troia

MISURE DI CONTROLLO DEL RISCHIO

Vengono illustrate le possibili misure di controllo per i rischi identificati al punto precedente, distinguendo tra misure fisiche, elettroniche e procedurali.

Verranno dettagliate nel seguito del documento le misure di controllo utilizzate per ogni singolo sito/sistema di trattamento.

Misure fisiche

- Sistema anti-intrusione del sito
- Sistema di rilevazione incendio

•

- Gruppo di continuità con protezione da sovratensioni
- Ambiente dotato di porta con chiave a distribuzione controllata
- Armadio con chiave a distribuzione controllata

Misure elettroniche

- Autenticazione con username/password univoca per utente
- Politica di controllo della robustezza delle password
- Controllo di accesso ai files/basi dati basato su ACL (access control list)
- Controllo di accesso ai programmi basato su ACL (access control list)
- Memorizzazione dei dati su server sicuri
- Firewall
- Crittografia dei dati trasmessi su rete pubblica
- Crittografia dei dati memorizzati su archivi elettronici
- Audit degli accessi al sistema
- Sistema di backup automatico su supporto rimovibile
- Antivirus

Misure procedurali

- Linee guida di utilizzo del SIA
- Linee guida per la memorizzazione dei dati su supporto magnetico
- Linee guida per la memorizzazione dei dati su supporto cartaceo
- Distinzione dei ruoli tra utenti e amministratori del sistema
- Linee guida per la messa in esercizio e la dismissione dei sistemi informatici
- Procedura di backup/recovery dei dati sul server
- Procedure di audit periodico dei sistemi

•

MISURE DI SICUREZZA ITEM S.R.L..

Si riportano di seguito le misure di sicurezza connesse al sistema di trattamento dati di ITEM S.R.L...

Misura da verificare	Cadenza della verifica	Periodicità
Reimpiego dei supporti di memorizzazione	Controlli sulla ricuperabilità delle informazioni precedentemente contenute	Sempre
Piano di formazione	Controlli periodici	Annuale
Restrizioni di accesso per via telematica	Controlli periodici	Annuale
Sicurezza delle trasmissioni di dati	Controlli periodici	Annuale
Criteri e procedure per assicurare l'integrità dei dati	Controlli periodici	Annuale
Controllo accesso delle persone autorizzate ai locali	Controlli periodici	Annuale
Protezione delle aree e dei locali	Controlli periodici	Annuale
Analisi delle responsabilità	Controlli periodici	Annuale
Analisi delle distribuzioni dei compiti	Controlli periodici	Annuale
Analisi dei rischi	Controlli periodici	Annuale
Validità richiesta di accesso ai dati personali	Verificata prima di consentire l'accesso stesso	Sempre
Autorizzazioni all'accesso	Almeno una volta all'anno, è verificata la sussistenza delle condizioni per la loro conservazione	Annuale
Autorizzazioni all'accesso	Rilasciate e revocate periodicamente	Sempre
Antivirus	Efficacia ed aggiornamento sono verificati con cadenza almeno semestrale	6 mesi
Codici identificativi personali	Disattivazione in caso di mancanza di utilizzo dei medesimi per un periodo superiore ai 6 mesi	6 mesi
Codici identificativi personali	Disattivazione in caso di perdita della qualità che consentiva l'accesso all'elaboratore	Sempre
Variazione programmata parola chiave	Per dati comuni a cadenza semestrale deve essere avviata la procedura per il cambio della parola chiave	6 mesi
Variazione programmata parola chiave	Per dati sensibili a cadenza trimestrale deve essere avviata la procedura per il cambio della parola chiave	3 mesi
Salvataggio dei dati	Salvataggio dei dati con frequenza almeno mensile	1 mese