MANUALE PRIVACY

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016

Data	Rev.	Oggetto revisione	Resp. Redazione	Resp. Approvazione
23/10/2018	0	Prima emissione	Titolare del Trattamento	Titolare del Trattamento

INDICE

0. PREMESSA

A.C.I. Promoter srl è società in house dell'AC Viterbo, e pertanto svolge la propria attività solo ed unicamente per l'Ente.
Le strumentazioni ed i software sono dati in dotazione ai dipendenti della società per lo svolgimento dei servizi istituzionali e risultano di proprietà dell'AC Viterbo, ovvero di ACI e ACI Informatica Spa. L'immobile ove ha sede **A.C.I. Promoter srl** è di proprietà dell'AC Viterbo. I sistemi di sicurezza antincendio sono installati e manutenuti dell'Ente, così come l'arredamento e le altre dotazioni necessarie allo svolgimento delle attività.

1. SCOPO

Il presente Manuale è redatto in conformità al Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio (GDPR), in particolare sulla base di quanto disposto dall'art. 32 in merito alla *valutazione dei rischi nel trattamento dati e alle misure tecniche organizzative adeguate per garantire un livello adeguato di sicurezza*.

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, la **A.C.I. Promoter srl** (d'ora in avanti anche Azienda)**,** in qualità di *Titolare* del trattamento dei dati personali mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al regolamento Europeo sulla protezione dei dati.

In considerazione di quanto sopra, gli obiettivi primari del presente Documento sono i seguenti:

- Migliorare la consapevolezza dei rischi insiti nel trattamento dei dati con l'ausilio di strumenti elettronici, con particolare riferimento alla gestione e all'utilizzo del sistema informativo ed effettuare una valutazione di rischio sui trattamenti dei dati personali dell'azienda;
- Individuare e definire adeguate misure tecniche ed organizzative finalizzate alla salvaguardia, alla corretta gestione e al corretto utilizzo del patrimonio informativo aziendale;
- Adottare idonei presidi di controllo al fine di contenere i rischi, prevenendo le possibili situazioni di pericolo;

- Fornire adeguate istruzioni comportamentali e procedurali ai soggetti coinvolti nella gestione dei singoli trattamenti (soggetti autorizzati).

Per il raggiungimento dei suddetti obiettivi la **A.C.I. Promoter srl** pone in essere, fra l'altro, le seguenti attività:

- Raccolta dei trattamenti effettuati e delle banche dati gestite, al fine di individuare le diverse tipologie di dati trattati, i rischi potenziali e le conseguenti misure di sicurezza (art. 32 Reg.);
- Redazione di un Manuale Privacy che include regole deontologiche e misure minime di sicurezza attuate e previste dal nuovo Regolamento UE;
- Redazione di Registro delle attività del trattamento (**Allegato 1**) che include i riferimenti a:
  - Titolare (o responsabile del trattamento o del titolare per cui si agisce);
  - Descrizione delle attività effettuate dal titolare (o per conto del titolare);
  - Finalità del trattamento dei dati;
  - Base giuridica del trattamento;
  - Categorie di dati;
  - Soggetti autorizzati a trattare i dati;
  - Destinatari dei dati;
  - Misure di sicurezza adottate;
  - Termini per la cancellazione dei dati;
  - Destinatari UE e Extra UE

2. TERMINI E DEFINIZIONI

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
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
LIMITAZIONE DI TRATTAMENTO	Il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
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
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
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
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
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
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
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
VIOLAZIONE DEI DATI PERSONAL /DATA BREACH	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
DATA 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
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
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
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 regolamento
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 regolamento
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
GRUPPO IMPRENDITORIALE	Un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate
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
AUTORITÀ DI CONTROLLO	L'autorità pubblica indipendente istituita da uno stato membro ai sensi dell'articolo 51 del regolamento
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
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
OBIEZIONE PERTINENTE E MOTIVATA	Un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al 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
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
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

3. DIRITTI DELL'INTERESSATO

3.1 Comunicazione con l'interessato

L'azienda ha adottato misure appropriate per fornire all'interessato tutte le informazioni e le comunicazioni relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. Le informazioni sono fornite per iscritto o con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

3.2 Dati raccolti presso l'interessato

L'azienda raccoglie presso l'interessato i dati che lo riguardano, e allo stesso fornisce, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:

- L'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
- I dati di contatto del responsabile della protezione dei dati, ove applicabile;
- Le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- I legittimi interessi perseguiti dal titolare del trattamento o da terzi (quando applicabile);
- Gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- Ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibilità.
- Il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- L'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
- L'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- Il diritto di proporre reclamo a un'autorità di controllo;
- Se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se

l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
- L'esistenza di un processo decisionale automatizzato, compresa la profilazione, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato

Tale informazioni sono fornite all'interessato attraverso la sottoposizione allo stesso del modello di informativa e consenso (Allegato 3, Allegato 4, Allegato 4.1).

4. MODALITA DI TRATTAMENTO DEI DATI

4.1 Natura dei dati trattati dall'Azienda

L'azienda tratta o può trattare i dati personali:
- Dei propri dipendenti,
- Di utenti e clienti che usufruiscono dei servizi istituzionali e commerciali erogati,
- Dati di terzi collaboratori, compresi i fornitori.

I dati trattati possono essere sia i dati anagrafici/identificativi che dati particolari (in particolare per i dipendenti, per gli utenti e per i clienti).

Le tipologie di dati trattati saranno esemplificate nell'apposito registro dell'attività di trattamento (Allegato 1), unitamente alle finalità e a tutte le altre informazioni richieste dal Regolamento.

4.2 Responsabile del Trattamento

Il titolare del trattamento ha deciso di ricorrere ad un responsabile del trattamento che presenti garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del regolamento e garantisca la tutela dei diritti dell'interessato.
In particolare, ai sensi dell'art. 28 REG. UE 2016/679, il Responsabile del trattamento si impegna a:
a) trattare i dati personali soltanto su istruzione documentata dell'azienda, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento dovrà informare la **A.C.I. Promoter srl** circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

b) garantire che i dipendenti incaricati, ovvero le persone autorizzate al trattamento dei dati personali, si siano a loro volta impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
c) adottare tutte le misure di sicurezza richieste;
d) rispettare le condizioni dal regolamento europeo per ricorrere a un altro responsabile del trattamento;
e) assistere il titolare del trattamento, tenendo conto della natura del trattamento, con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo dell'azienda di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III REG. UE 2016/679;
f) assistere la **A.C.I. Promoter srl** nel garantire il rispetto degli obblighi previsti, tenendo conto della natura del trattamento e delle informazioni a Sua disposizione;
g) cancellare o restituire, su scelta dell'azienda tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;
h) mettere a disposizione dell'azienda tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzati dalla **A.C.I. Promoter srl** da un altro soggetto da questi incaricato;
i) informare immediatamente l'azienda qualora, a suo parere, un'istruzione violi il regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

Il responsabile del trattamento provvede ad organizzare le mansioni in modo tale, che agli interessati del trattamento venga data pronta soddisfazione nell'esercizio dei loro diritti.

Per il Responsabile del trattamento interno è stata predisposta un'apposita lettera di nomina (Allegato 5.1).
Gli obblighi in materia di protezione dei dati previsti per i Responsabili del trattamento esterni sono riportati nell'Allegato 5.2 o comunque nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento.

4.3 Designazione delle persone autorizzate

Il titolare del trattamento indica le persone autorizzate all'interno dell'azienda. Ogni operatore che agisce sotto l'autorità della **A.C.I. Promoter srl** o del Responsabile è autorizzato al trattamento dei dati derivanti dall'espletamento dei compiti e delle funzioni ad esso attribuiti e dal profilo abilitativo assegnato, in conseguenza della sua preposizione ad una determinata unità operativa, risultante dalla relativa lettera di incarico (Allegato 6 Atto di autorizzazione al trattamento dei dati).

4.4 Attività delle persone autorizzate

Gli "*autorizzati*", nel trattare i dati personali, dovranno operare garantendo la massima riservatezza delle informazioni di cui vengono in possesso. Dovranno considerare tutti i dati personali come confidenziali e, di norma, soggetti al segreto d'ufficio, fatta eccezione per i soli dati anonimi, generalmente trattati per elaborazioni statistiche, e per quelli acquisibili da chiunque perché contenuti in atti, liste ed elenchi pubblici (che non rilevano ai fini del Regolamento UE).

4.5 Procedure operative

Le procedure di lavoro, le prassi operative e la condotta tenuta nello svolgimento delle operazioni di trattamento, dovranno mirare ad evitare che:

- I dati personali siano soggetti a rischi di distruzione o perdita anche accidentale;
- I dati possano accedere persone non autorizzate;
- Vengano svolte operazioni di trattamento non consentite o non conformi ai fini per i quali i dati stessi sono stati raccolti.

Deve, quindi, sempre garantirsi l'integrità del dato, la sua disponibilità e la sua confidenzialità.
Il personale autorizzato dovrà perciò operare con la massima diligenza ed attenzione in tutte le fasi di trattamento: dalla esatta acquisizione dei dati, all'eventuale loro aggiornamento; così per la conservazione, la custodia ed eventuale cancellazione o distruzione.
Le persone autorizzate non potranno pertanto eseguire operazioni di trattamento per fini non previsti tra i compiti loro assegnati e comunque riferiti alle disposizioni e regolamenti vigenti nell'azienda.

In seguito a quanto emerso dall'effettuazione del censimento dei trattamenti di dati personali e dall'analisi dei rischi, si stabilisce quanto segue:

- I dati particolari (ex dati sensibili) potranno essere trattati esclusivamente dai soggetti all'uopo individuati ed autorizzati;

- Ogni altra persona autorizzata al trattamento di dati particolari (ex sensibili), diverso dai soggetti indicati al precedente punto dovrà ricevere specifiche indicazioni scritte o verbali che integrano quelle generali previste dal regolamento;

- Il personale autorizzato che svolge operazioni di trattamento di dati particolari (ex sensibili), utilizzando elaboratori, è autorizzato altresì all'accesso agli strumenti abilitati per tali trattamenti, all'accesso ai locali in cui vengono svolte tali lavorazioni ed alle operazioni di trattamento, e dovrà attenersi alle norme

di sicurezza stabilite dall'azienda per tali trattamenti.

5. POLICY AZIENDALE PER I TRATTAMENTI SVOLTI CON STRUMENTI ELETTRONICI E/O AUTOMATIZZATI

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet dai Personal Computer e dalle applicazioni, espone la **A.C.I. Promoter srl** e gli interessati (dipendenti e collaboratori della stessa), a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto d'autore e Regolamento Europeo sulla protezione dei dati, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine dell'azienda stessa.
Premesso quindi che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, l'azienda adotta una specifica Policy con l'obiettivo di evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati. Le prescrizioni previste si aggiungono ed integrano le disposizioni del nuovo regolamento europeo sulla protezione dei dati personale (Reg. UE 679/2016), nonché integrano le informazioni già fornite agli interessati in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse. A tal fine è stata elaborata e messa a disposizione di dipendenti e collaboratori una istruzione operativa **"IO 01 - Policy aziendale per trattamenti elettronici e/o automatizzati".** Le disposizioni in essa contenute sono oggetto di formazione continua del personale almeno con cadenza annuale.

6. POLICY AZIENDALE PER I TRATTAMENTI SVOLTI CON STRUMENTI DIVERSI DA QUELLI ELETTRONICI E/O AUTOMATIZZATI

Il personale debitamente autorizzato al trattamento dei dati con strumenti diversi da quali elettronici e/o automatizzati, con particolare riferimento alla gestione cartacea di documento contenenti dati personali, dovrà seguire le istruzioni impartite dal titolare del trattamento. A tal fine è stata elaborata e messa a disposizione di dipendenti e collaboratori una istruzione operativa **"IO 02 - Policy aziendale per trattamenti su supporti cartacei".** Le disposizioni in essa contenute sono oggetto di formazione continua del personale almeno con cadenza annuale.

7. NATURA DEI DATI E TIPOLOGIE DI TRATTAMENTO

7.1 Natura dei dati trattati

L'azienda può trattare diverse tipologie di dati.

Di seguito un elenco sintetico delle tipologie di dati trattati:

Dipendenti /Collaboratori	Dati personali e identificativi Dati particolari (es. Relativi alla salute dei lavoratori e alle iscrizioni al sindacato) Dati giudiziari
Clienti	Dati e anagrafiche aziendali (che non si configurano come dato personale) Dati personali e identificativi Dati giudiziari (ad. es. dati relativi a sentenze di separazione, a debiti tributari e fermi amministrativi) Dati sanitari relativi alle esenzioni bollo per disabili (verbali disabilità Legge 104 senza omissis) e certificati medici per attività sportiva agonistica
Fornitori	Dati e anagrafiche aziendali (che non si configurano come dato personale) Dati personali e identificativi acquisiti nella gestione del rapporto contrattuale

Un elenco esaustivo è contenuto all'interno del Registro delle attività di trattamento (Allegato 1).

7.2 Modalità di Trattamento

I dati di dipendenti/collaboratori, dei clienti e dei fornitori sono trattati in formato cartaceo ed in formato elettronico.
Si rimanda alla **"IO 01 - Policy aziendale per trattamenti elettronici e/o automatizzati"** e alla **"IO 02 - Policy aziendale per trattamenti su supporti cartacei"** per tutti i dettagli.

7.3 Registro dei trattamenti

La **A.C.I. Promoter srl** ha istituito un registro delle attività di trattamento (Allegato 1) svolte sotto la propria responsabilità che contiene le seguenti informazioni:

a) il *nome e i dati di contatto del titolare del trattamento* e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;

b) le finalità del trattamento;

c) una descrizione delle categorie di interessati e delle categorie di dati personali;

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.

7.4 Integrità dei Dati

Le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile hanno accesso ai soli dati personali la cui conoscenza è strettamente necessaria per adempiere ai compiti loro assegnati e si attengono alle istruzioni impartite.

8. MODALITA' DI ACCESSO AI DATI

Gli accessi al sistema informativo aziendale ed agli archivi documentali cartacei avvengono esclusivamente secondo modalità prestabilite.
I soggetti autorizzati al trattamento dei dati ricevono le abilitazioni in modo da poter

accedere ai soli dati necessari per l'espletamento delle mansioni assegnate.

Si rimanda alla **"IO 01 - Policy aziendale per trattamenti elettronici e/o automatizzati"** e alla **"IO 02 - Policy aziendale per trattamenti su supporti cartacei"** per tutti i dettagli.

9. CRITERI E MODALITÀ DI RIPRISTINO DELLA DISPONIBILITÀ DEI DATI

Il piano di continuità operativa rappresenta l'aspetto della sicurezza principalmente orientata a garantire la continuità e la disponibilità dei sistemi informativi automatizzati rispetto a danneggiamenti causati da eventi accidentali, sabotaggi e disastri naturali.

L'infrastruttura informatica di **A.C.I. Promoter srl** è fornita e gestita da AC Viterbo tramite la società incaricata ACI Informatica SpA. AC Viterbo, in qualità di ente pubblico, ha predisposto le misure minime di sicurezza previste nella Circolare AgID del 18 aprile 2017, n. 2/2017 ("Misure minime di sicurezza ICT per le pubbliche amministrazioni "). Si rimanda al "Modulo di implementazione delle misure minime di sicurezza dell'Automobile Club Viterbo", allegato al presente Manuale, per i dettagli circa:

- Inventario dei dispositivi autorizzati e non autorizzati
- Inventario dei software autorizzati e non autorizzati
- Protezione delle configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server
- Valutazione e correzione continua della vulnerabilità
- Uso dei privilegi di amministratore
- Difese contro i malware
- Copie di sicurezza
- Protezione dei dati

Vengono inoltre poste in essere procedure idonee a garantire l'organizzazione e la custodia della documentazione digitale e cartacea gestita dall'azienda in archivi elettronici e fisici ad accesso autorizzato e sotto il diretto controllo del Titolare/Responsabile del trattamento, come dettagliato nelle istruzioni operative redatte (**"IO 01 - Policy aziendale per trattamenti elettronici e/o automatizzati"** e **"IO 02 - Policy aziendale per trattamenti su supporti cartacei"**).

10. MISURE DI SICUREZZA IN CASO DI TRATTAMENTO DI DATI PERSONALI AFFIDATI A TERZI

Qualora il trattamento dei dati debba essere effettuato per conto del Titolare, quest'ultimo deve avere tutte le garanzie che il trattamento si svolga secondo i requisiti del Regolamento e garantisca la tutela degli interessati.
I trattamenti da parte dei **Responsabili esterni** sono disciplinati mediante un contratto (anche lo stesso contratto di servizi) o addendum contrattuale che prevede che il soggetto cui le attività sono affidate si impegni a (art. 32 del Reg.):

- Trattare i dati personali soltanto su istruzione documentata del titolare del trattamento anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento dovrà informare titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
- Garantire che le persone autorizzate al trattamento dei dati personali si siano a loro volta impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- Adottare tutte le misure di sicurezza richieste;
- Assistere il titolare del trattamento, tenendo conto della natura del trattamento, con misure tecnico organizzative adeguate, nella misura di cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;
- Assistere il titolare del trattamento nel garantire il rispetto degli obblighi previsti dal regolamento europeo, tenendo conto della misura del trattamento;
- Cancellare o restituire, su scelta del titolare del trattamento tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;
- Mettere a disposizione del titolare del trattamento di tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato. Si impegna ad informare senza ritardo il titolare del trattamento qualora, a suo parere, un'istruzione violi il Regolamento o altre disposizioni, nazionali o dell'Unione, relativa alla protezione dei dati.

Sono previste verifiche periodiche da parte del Titolare presso i Responsabili esterni all'Azienda in merito al rispetto delle disposizioni in materia di trattamento, compreso il profilo della sicurezza. Le clausole contrattuali stipulate con i Responsabili esterni contengono un protocollo per l'effettuazione delle suddette verifiche.

11. MISURE DI SICUREZZA TECNICHE: MISURE INFORMATICHE, CARTACEE E LOGISTICHE E SISTEMI DI VIDEOSORVEGLIANZA

In generale, un sistema informativo si definisce sicuro quando soddisfa i seguenti requisiti:

- **Disponibilità**: l'informazione ed i servizi che eroga devono essere disponibili per gli utenti coerentemente con i livelli di servizio;
- **Integrità**: l'informazione ed i servizi erogati possono essere creati, modificati, o cancellati solo dalle persone incaricate a svolgere tale operazione;
- **Confidenzialità o Riservatezza**: l'informazione può essere utilizzata solo dalle persone incaricate a compiere tale operazione.
- **Custodia e controllo:** i dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non conforme alle finalità della raccolta.

11.1 Verifiche periodiche sulle misure di sicurezza informatiche, cartacee e logistiche

Si rimanda al "Modulo di implementazione delle misure minime di sicurezza dell'Automobile Club Viterbo", allegato al presente Manuale, per tutti i dettagli.

11.2 Descrizione del sistema informatico

A.C.I. Promoter srl dispone della seguente architettura hardware:

- N. 7 PC collegati alla rete Intranet attraverso un router IMOLA fornito da ACI per il tramite di ACI Informatica S.p.A. (n. 1 dispositivo di questi è collegato alla rete in modalità Wi-Fi)
- N. 3 POS per pagamenti con moneta elettronica, di cui n.2 POS/ACI – N.1 POS/AC Viterbo

11.3 Videosorveglianza: valutazione sulle necessità e finalità del trattamento

Allo stato attuale non risulta installato presso la sede di **A.C.I. Promoter srl** alcun sistema di videosorveglianza.

11.5 Descrizione sistemi di rilevazione presenze

Presso la sede non sono presenti sistemi automatizzati di raccolta delle presenze.

11.6 Archivi cartacei

Tutta la documentazione cartacea viene raccolta in schedari/archivi chiusi a chiave. Si rimanda alla **IO 02 - Policy aziendale per trattamenti con supporti cartacei** per tutti i dettagli.

12. VALUTAZIONE DEL RISCHIO

12.1 Metodologia

Di seguito è riportata la procedura utilizzata per la determinazione del rischio e delle misure di mitigazione associate al trattamento di dati personali all'interno dell'azienda.

Per ciascuna tipologia di dato/informazione da preservare, sono state definite tramite:

- Le necessità di protezione in termini di Riservatezza, Integrità, Disponibilità;
- Le politiche di carattere generale atte a garantire i suddetti principi;
- I soggetti coinvolti nell'applicazione di tali politiche, comprendendo anche i soggetti terzi interessati.

Il modello metodologico di riferimento per effettuare l'Analisi dei Rischi promuove un approccio orientato ai processi ed adotta il modello PDCA per il suo mantenimento. Il processo di analisi e gestione dei rischi si pone all'interno della fase di Plan e prevede:

- Definizione dell'approccio e della metodologia adottata per la valutazione del rischio, lo sviluppo di criteri per accettare i rischi e l'identificazione dei livelli accettabili di rischio;
- Identificazione dei rischi definendo:
    - I dati personali e gli owner\uffici di riferimento;
    - Gli impatti che la perdita di riservatezza, integrità e disponibilità può avere sui dati.
    - Le minacce che incombono sui dati personali;

- Le vulnerabilità che possono essere sfruttate da tali minacce;

- Analisi e la valutazione dei rischi: processo sistematico per identificare le cause e stimare l'impatto che i rischi possono avere sul dato personale aziendali, valutando la probabilità di occorrenza di un evento negativo (alla luce delle minacce e vulnerabilità identificate). Il risultato di tale processo è identificato con un valore di rischio e dalla necessità o meno di trattamento dello stesso;
- Gestione dei rischi: si intende l'identificazione e ponderazione delle opzioni per il trattamento dei rischi (applicazione degli appropriati controlli, accettazione dei rischi in modo consapevole, modalità per evitare i rischi);
- Identificazione degli obiettivi di controllo e dei controlli per il trattamento dei rischi.
- Il conseguimento dei risultati previsti e il miglioramento continuo attraverso la prevenzione o la riduzione degli effetti indesiderati provocati dall'evento negativo.

In fase di rivalutazione periodica è previsto che venga effettuato un monitoraggio (Check) che richiede la revisione della valutazione dei rischi a intervalli prestabiliti, dei rischi residui e dei livelli di rischio residuo accettabile ed identificabile, tenendo in considerazione i cambiamenti intervenuti all'interno dell'organizzazione.

12.2 Risultati e Benefici della Valutazione dei Rischi

Lo scopo principale dell'analisi e gestione dei rischi in questo contesto è quello di individuare le cause di possibili situazioni che possono rappresentare un pericolo per la sicurezza delle informazioni personali.
Pertanto, l'analisi dei rischi può essere utilizzata come un importante strumento per indirizzare correttamente gli investimenti aziendali in materia di sicurezza. La simulazione attraverso il calcolo del valore di rischio per un determinato dato personale, a seguito dell'applicazione di un eventuale controllo, fornisce, infatti, un'indicazione per bilanciare i benefici per la sicurezza con il costo necessario per l'implementazione di una determinata contromisura.

I benefici della gestione dei rischi sono:

- **Garantire la compliance agli aspetti cogenti, a norme e regolamenti di settore in materia di sicurezza.**

Es. la tutela della privacy regolamentata dal Regolamento UE 2016/679

- **Assicurare la continuità del business.**

Intesa come assicurazione della continuità dei servizi erogati ai clienti anche in caso di evento inatteso che può compromettere le operazioni di business e di minacciare la sicurezza delle informazioni (Security).

- **Minimizzare i danni.**

Attuazione delle contromisure mirate all'abbattimento (parziale o totale) del livello di rischio associato ad un determinato incidente di sicurezza.

12.3 Analisi dei rischi

Vantaggi dell'approccio preventivo per l'analisi dei rischi

L'analisi dei rischi costituisce un elemento essenziale nell'ambito della componente di Governance relativa alla sicurezza dei dati personali; assicura che i sistemi di protezione progettati e attuati siano coerenti con le minacce pertinenti e le relative probabilità di accadimento, nonché con le vulnerabilità esistenti.
A differenza dell'approccio reattivo alla gestione del rischio, che è basato sulla risoluzione degli incidenti di sicurezza, quindi dopo che questi si sono verificati, l'approccio preventivo mira ad individuare anticipatamente le contromisure atte a ridurre la probabilità che gli incidenti si verifichino.

Riservatezza, Integrità e Disponibilità

Al fine di valutare correttamente i risultati della valutazione dei rischi, vengono fornite le definizioni di Riservatezza, Integrità e Disponibilità (R.I.D.) sia in relazione alla definizione fornita dalla norma UNI ISO/IEC 27001:2005 sia in relazione alle violazioni dei dati personali:

- ***Riservatezza***: esprime la proprietà per cui una determinata informazione non sia resa disponibile o comunicata a individui, entità processi, applicazioni e utenti non autorizzati, sia in modo intenzionale, sia in modo accidentale.
- ***Integrità***: esprime la proprietà che l'informazione sia accurata e completa e cioè che non subisca alterazioni non autorizzate, siano esse accidentali o intenzionali.
- ***Disponibilità***: esprime la proprietà che l'informazione sia accessibile e utilizzabile su richiesta di un'entità autorizzata e che i soggetti autorizzati possano effettivamente accedere alle informazioni ogniqualvolta sia necessario, anche in presenza di eventi che possano sia accidentalmente che deliberatamente impedirne l'accesso.

I dati devono essere trattati in modo 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.

Caratteristiche del metodo

La metodologia adottata per la valutazione dei rischi permette di determinare il rischio associato a ciascun dato personale sia in termini assoluti (quando l'analisi viene condotta per la prima volta in assenza di contromisure) che in termini di rischio residuo (nelle valutazioni successive che tengono conto delle contromisure poste in essere).

Essendo già in atto delle contromisure, la reiterata applicazione dell'analisi del rischio darà invece una misura dell'efficacia (in termini di riduzione del rischio residuo) delle contromisure via via adottate.

I rischi dei singoli dati personali sono valutati considerando innanzitutto il loro valore intrinseco (classificazione), successivamente si procede all'identificazione delle minacce che possono pregiudicare la riservatezza, l'integrità o la disponibilità delle informazioni gestite, considerando qual è la probabilità che esse possano sfruttare le vulnerabilità definite. Successivamente si valuta quale potrebbe risultare l'impatto derivante dal concretizzarsi della minaccia in a seguito di una mancanza di riservatezza, integrità o indisponibilità. Infine si determina quale sarebbe il danno conseguente dalla perdita di informazioni e, quindi, si può procedere con la valutazione del rischio, ottenuto dal prodotto dei fattori adoperati per la valutazione.
La valutazione dei rischi produce come risultato un valore che viene associato in maniera diretta al dato personale preso in esame ed alla minaccia che può concretizzarsi.

E' possibile aggiornare il set di minacce e vulnerabilità in relazione all'evolversi del contesto tecnologico e dei requisiti di business aziendali.

In seguito alla valutazione dell'accettabilità del rischio si procede con la definizione delle contromisure, che sono selezionate in base alla gravità del rischio e quindi in relazione al loro peso complessivo nell'abbattimento del rischio. La valutazione di selezione di una contromisura più che un'altra risulta influenzata da differenti parametri come costo, grado di efficacia, assenza di misure alternative.

Definizioni

Rischio	Eventualità che una minaccia possa trasformarsi in danno reale, determinando un impatto
Sicurezza dell'informazione	Mantenimento di disponibilità, integrità e riservatezza dell'informazione: possono essere inoltre coinvolte altre proprietà quali autenticità, responsabilità, non ripudio e affidabilità
Incidente di sicurezza	Evento o serie di eventi di sicurezza dell'informazione non voluti o inattesi che hanno un probabilità significativa
Rischio potenziale (intrinseco)	Livello di esposizione ad una minaccia messo in relazione alla criticità di un determinato dato personale

Rischio effettivo (residuo)	Rischio che rimane dopo il processo di trattamento dei rischi, ovvero livello di rischio che tiene conto delle contromisure implementate. Il rischio residuo si differenzia dal rischio in assoluto (precedente all'applicazione delle contromisure), perché misura il livello di rischio "attuale"; il rischio residuo confrontato con il rischio precedente all'applicazione delle contromisure può quindi costituire un sistema per misurare l'efficacia stimata della contromisura in questione
Accettazione del Rischio	Decisione di accettare un rischio
Analisi dei Rischi	Uso sistematico di informazioni per identificare le cause e stimare il rischio
Valutazione dei Rischi	Processo complessivo di analisi e ponderazione dei rischi
Ponderazione dei Rischi	Processo di comparazione dei rischi stimati con criteri di rischio dati al fine di determinare la significatività del rischio
Gestione dei Rischi	Insieme di attività coordinate per dirigere e controllare un'organizzazione rispetto ai rischi
Trattamento dei Rischi	Processo riguardante la selezione e l'implementazione di misure per modificare il livello di rischio
Minaccia	Evento di natura dolosa o accidentale che, sfruttando una vulnerabilità del sistema, potrebbe provocare danno
Vulnerabilità	Debolezza intrinseca o dovuta a condizioni di esercizio che possa essere sfruttata da una minaccia per arrecare danno. Nel modello adottato viene evidenziato anche il concetto di assenza di controlli; ciò permette di effettuare la misurazione del rischio effettivo o residuo
Danno	Conseguenza negativa dell'attuarsi di una minaccia
Impatto	Effetto sull'azienda e sul suo business del verificarsi di una minaccia, ovvero l'effetto reale del danno sul sistema (può tener conto anche di possibili responsabilità civili o penali o della perdita di autorizzazioni o riconoscimenti)

12.4 Processo per l'analisi e la gestione dei rischi – Descrizione delle fasi

Il processo di analisi e gestione del rischio è articolato nelle fasi di seguito riportate:

Classificazione del dato personale

Tale fase prevede l'identificazione del valore dei singoli dati personali (categorie) rispetto all'impatto causato da un'eventuale perdita di riservatezza, disponibilità ed integrità degli stessi. La classificazione riflette l'importanza dei dati personali attribuita dal management e dal Regolamento Europeo sul trattamento dei dati personali, in tal senso si può stabilire una diretta dipendenza fra i risultati dell'analisi del rischio e gli obiettivi di sicurezza stabiliti nelle politiche. Il valore del dato personale così determinato costituisce la prima variabile in input per il calcolo del livello di Rischio.

Ubicazione	Sede fisica e informatica del dato personale
Owner	Soggetto autorizzato e/o Responsabile del trattamento del dato
Classificazione	Attribuita al dato personale scegliendo tra i valori definiti in fase di classificazione;
Minacce	Valore impatto della minaccia su RID
Probabilità di accadimento	Valore di probabilità di accadimento per le vulnerabilità del dato personale
Vulnerabilità	Valore più alto delle probabilità di accadimento delle singole categorie di vulnerabilità
Impatto globale	Somma di impatti delle le minacce × classificazione del dato personale
Danno	Valore del danno
Rischio	Valore del danno × probabilità di accadimento delle vulnerabilità
Livello di rischio	Scala numerica di livello di rischio
Rischio accettabile	Valore di rischio.

Tramite questa relazione è possibile periodicamente ridefinire il livello di rischio e la criticità all'interno del perimetro preso in considerazione.
Il risultato è ricalcolabile a distanza di tempo, garantendo la ripetibilità della valutazione dei rischi, nonché la sua oggettività in base ai valori di ingresso.
Il rischio, inteso come misura dell'esposizione di un sistema ad impatti, minacce e vulnerabilità, è una grandezza derivata dalle seguenti tre variabili:

- Livello di classificazione del dato personale
- Vulnerabilità associata alla minaccia.
- Impatto della Minaccia
- Danno conseguente

Classificazione del dato personale e livelli di cautela da adottare

La scala di punteggi che determina il livello di importanza del dato personale in termini qualitativi (in base all'impatto derivante da una sua temporanea indisponibilità) è definita su una scala a cinque livelli, poi convertita numericamente. Di seguito viene fornita la scala di valori con la relativa descrizione di impatto.
I livelli di cautela da adottare per predisporre misure di sicurezza idonee varia a seconda della tipologia dei dati che vengono trattati. In particolare vengono adottate misure che assumono carattere di importanza crescente a seconda che si tratti di:

- Dati personali comuni
- Dati patrimoniale\economici (dati semi-sensibili)
- Dati riguardanti il ceto sociale, l'appartenenza politica, appartenenza sindacale, dati giudiziari (sensibili\particolari), dati biometrici, dati genetici, etc.

Nella seguente matrice si procede a una stima del grado di rischio insita nella tipologia dei dati trattati dal Titolare in particolare classificando il grado di pericolosità in:

- **Basso**: dati comuni – informazioni e dati personali classificabili come PUBBLICI
- **Medio**: dati particolari (ex sensibili) del personale interno/collaboratori – informazioni e dati personali classificabili come a USO INTERNO
- **Alto**: dati semi-sensibili / dei clienti – informazioni e dati personali classificabili come CONFIDENZIALI
- **Altissimo**: dati particolari di cui all'art. 9 e 10 – informazioni e dati personali classificabili come RISERVATI

PERICOLOSITA' PER LA PRIVACY DELL'INTERESSATO E IMPATTO IN TERMINI DI DANNO ALL'INTERESSATO E REPUTAZIONE AZIENDALE			
BASSO – VALORE 1	**MEDIO- VALORE 2**	**ALTO- VALORE 3**	**ALTISSIMO- VALORE 4**
Dati anagrafici comuni del personale interno	Dati relativi al personale idonei a rilevare l'adesione a sindacati o organizzazioni a carattere sindacale e lo stato di salute Dati relativi a sanzioni e provvedimenti disciplinari al personale (non presenti ad oggi)	Dati patrimoniali di clienti	Dati di cui all'art. 9 e 10 Non presenti
Dati comuni anagrafici relativi ai clienti: nome, cognome, indirizzi, P.IVA, codice	Dati comuni relativi ai candidati all'assunzione in qualità di dipendenti/collaboratori		

fiscale, telefoni, mail, coordinate bancarie			
Dati comuni relativi alla gestione fornitori: nome, cognome, ragione sociale, codice fiscale, indirizzo, mail, recapiti telefonici			

Ai fini del calcolo del livello di rischio, sarà preso in considerazione il valore più alto tra quelli associati a ciascun parametro (Riservatezza, Integrità, Disponibilità).

12.5 Identificazione delle minacce e delle vulnerabilità che esse possono sfruttare.

La corretta identificazione delle minacce è un elemento di basilare importanza in quanto il valore del rischio calcolato viene valutato in relazione alla minaccia.

Le minacce identificate all'interno della metodologia di analisi dei rischi sono raggruppate secondo le seguenti categorie:

- Cancellazione
- Modifica
- Visualizzazione del dato da parte di soggetti non autorizzati
- Perdita
- Rapporto terzi
- Divulgazione non autorizzata (Comunicazione e diffusione)

Per ogni minaccia identificata viene quindi valutata la probabilità che essa possa sfruttare una delle vulnerabilità identificate. Esse sono suddivise in categorie e a ciascuna viene attribuito un valore numerico di probabilità di accadimento che tiene conto delle eventuali contromisure già implementate. La più alta di tali probabilità di accadimento determina la vulnerabilità complessiva del sistema in relazione alla specifica minaccia.

Le categorie di vulnerabilità individuate sono:

- Risorse umane
- Ambientale e fisica
- Gestione PC e reti

- Attività gestionali

Di seguito una tabella riepilogativa delle diverse vulnerabilità con la relativa descrizione.

CATEGORIA	VULNERABILITA'	DESCRIZIONE
Risorse umane e comportamento degli operatori	Comportamenti sleali o fraudolenti	Si riferisce al realizzarsi di un evento dannoso sul dato personale volontario da parte di un soggetto interno/esterno
	Disattenzione e incuria	Si riferisce all'insufficienza o alla mancanza di attenzione da parte del personale sul trattamento del dato personale
	Uso non corretto/conforme delle informazioni	Possibilità di utilizzo non corretto doloso o accidentale delle informazioni trattate dagli incaricati
	Errori materiali	Si riferisce a comportamenti che generano errori dovuti all'assenza o alla carenza di formazione / informazione sul corretto utilizzo dell'uso del dato personale
Ambientale e fisica	Dispositivi di memorizzazione removibili non protetti	Dispositivi di memorizzazione o back up non protetti da furti, violazioni, manomissioni, modificazioni e danneggiamenti. La protezione si intende fisica
	Suscettibilità degli apparati all'umidità/temperatura/sbalzi di alimentazione elettrica	Grado di sensibilità ed eventuale intolleranza degli apparati ad operare a livelli massimi e minimi di percentuale di umidità, di temperatura, fluttuazione corrente elettrica.
	Impossibilità di accesso agli uffici	Caso in cui per qualunque motivo non è possibile accedere ai locali
	Mancata protezione fisica degli archivi	Si riferisce agli armadi in cui sono archiviati documenti significativi
	Assenza controlli accesso fisico	Mancanza di controlli per gli accessi alle persone negli uffici e nei luoghi di lavoro.
Gestione PC e reti e strumenti di lavoro	Linee di comunicazione non protette	Si riferisce alla scarsità o assoluta mancanza di sistemi di protezione delle linee di comunicazioni (wireless etc.)
	Gestione delle password per l'accesso ai SW e ai PC non sicura	Si riferisce alla regola adottata per l'impostazione della password con il quale viene effettuato l'accesso ai sistemi
	Mancanza di protezione dei sistemi	Mancanza o inadeguatezza dei sistemi antivirus
	Mancanza gestione sovraccarico di rete	Si riferisce all'inadeguatezza di prevedere con anticipo e/o individuare tempestivamente l'aumento di richiesta di dati/informazioni in transito nei sistemi/apparati di rete, rispondendo con misure appropriate
	Connessioni a reti pubbliche non protette	Si intende l'assenza o la carenza di controlli sulle connessioni da e verso le reti pubbliche
	Bugs nei sistemi	Presenza di difetti e/o errori all'interno dei sistemi operativi che non sono indirizzati attraverso procedure organizzative ed operative collaudate in grado di applicare tempestivamente fix e patch

CATEGORIA	VULNERABILITA'	DESCRIZIONE
	Mancanza di logout automatici	Si riferisce all'assenza di controlli regole e configurazioni specifiche che consentono la terminazione automatica delle sessioni nel caso di inattività prolungata
Attività gestionali	Mancata cancellatura dei dispositivi riutilizzati	I casi in cui non venga prevista nessuna forma di cancellazione sicura dei dati dai dispositivi (dischi, memorie) dismessi e poi riutilizzati. Ciò potrebbe comportare una perdita involontaria di confidenzialità delle informazioni
	Mancanza di procedure operative documentate	Si riferisce alla mancanza o alla scarsità di documenti che dettaglino le procedure relative alla gestione, il controllo e la manutenzione, la revisione del monitoraggio dei sistemi e relative ai cambiamenti.
	Mancato controllo nella gestione del trasferimento delle informazioni con clienti e personale interno	Si riferisce allo scambio via e-mail tra azienda e clienti o tra colleghi
	SW applicativo non aggiornato	SW applicativo non adeguatamente supportato dai fornitori
	Specifiche di sicurezza incomplete	Mancanza o scarsità di specifiche di sicurezza incluse nei requisiti dei sistemi ed in generale nelle infrastrutture organizzative nelle fasi di gestione, controllo e manutenzione
	Mancanza di clausole di riservatezza nei contratti	Si riferisce alle condizioni aggiuntive da inserire nei contratti verso i fornitori e clienti

Per ogni minaccia viene quindi valutata la probabilità che essa possa sfruttare la vulnerabilità individuata e quindi comportare un danno alle informazioni gestite dal dato personale.

La probabilità viene determinata secondo il seguente criterio:

PROBABILITA'	VALORE	Descrizione
BASSA	1	Sono noti rarissimi episodi già verificatisi. L'azione della minaccia può provocare un danno solo in circostanze sfortunate di eventi.
MEDIA	2	E' noto qualche episodio in cui alla mancanza è di fatto seguito il danno. L'azione della minaccia può provocare un danno anche se non in modo automatico o diretto.
ALTA	3	Si sono verificati danni causati dalla minaccia in oggetto. L'azione della minaccia può provocare un danno anche se non associata ad altre circostanze

12.6 Identificazione dell'impatto

A questo punto si procede con la valutazione dell'impatto sulle attività aziendali conseguenti all'evento causato dalla minaccia. Vengono separatamente valutati gli

impatti in termini di riservatezza, integrità e disponibilità delle informazioni che vengono gestite attraverso il dato personale censito, secondo la seguente tabella.

- Riservatezza: il dato personale non deve essere esposto alla diffusione e comunicazione non autorizzato e alla visualizzazione da parte di soggetti non autorizzati:
- Integrità: il dato personale non deve essere esposto a modifiche, danni e/o cancellazioni non autorizzate
- Disponibilità: il dato personale non deve essere esposto alla perdita, danno, e/o alla cancellazione non autorizzate

Impatto	Valore
ALTO	3
MEDIO	2
BASSO	1

Tabella – Valorizzazione numerica dei livelli di impatto

Il valore dell'Impatto globale viene a sua volta calcolato secondo il seguente algoritmo:

Impatto globale = Val (IR) + Val (II) + Val (ID)

Dove
IR = Impatto su riservatezza
II = Impatto su integrità
ID = Impatto su disponibilità

12.7 Valutazione (Calcolo) del rischio

Il calcolo del Rischio viene effettuato mediante un algoritmo matematico che mette in relazione i valori precedentemente individuati.
Le variabili per il calcolo del rischio sono:

1. Classificazione del dato personale (valore aziendale)
2. Vulnerabilità del dato personale associata alla minaccia (probabilità che la minaccia possa sfruttare una vulnerabilità per causare un danno)
3. Impatto Globale della Minaccia (in termini di disponibilità, riservatezza, integrità,)
4. Valore relativo al danno (definito in valore numerico in relazione alla perdita di business).

Il valore numerico del rischio viene determinato dal prodotto dei quattro suddetti fattori, numericamente valorizzati.

Viene quindi determinato il livello di rischio, in funzione della seguente tabella:

Livello di rischio	DA	A
BASSO	0	34
MEDIO	35	68
ALTO	69	101
MOLTO ALTO	102	135

Identificazione del rischio accettabile

Con il termine rischio accettabile si intende il valore al di sotto del quale l'Azienda ritiene di non dover implementare contromisure di sicurezza volte alla riduzione del livello di rischio. L'identificazione del grado di rischio considerato come accettabile è compito del Management aziendale.

Sulla base del livello di rischio accettabile, vengono evidenziati i livelli di rischio uguali o superiori a quello accettabile, al fine di individuare qualitativamente l'esposizione al rischio del sistema o dato personale.

Il rischio accettabile viene definito dal livello di rischio BASSO e MEDIO e viene formalmente accettato dalla direzione dell'Organizzazione al fine di poter ottenere il corretto committment per procedere nella applicazione del piano di trattamento.

12.8 Risultati della valutazione del rischio

La classificazione del rischio cui sono esposti i singoli dati personali, in relazione alle minacce ipotizzate, consente di ottenere considerazioni oggettive nella valutazione. Ciò permette di attuare in maniera sistematica e ripetibile la valutazione stessa e quindi di identificare le opzioni per il trattamento scegliendo fra:

a) Mitigazione del rischio che consiste nell'applicazione di opportuni controlli;
b) Accettazione del rischio in modo consapevole, verificando che siano comunque soddisfatte le policy;
c) Elusione del rischio e cioè decidere di annullare il rischio reingegnerizzando i processi, evitando di trattare determinate informazioni, o certe soluzioni tecnologiche (se possibile);
d) Trasferimento del rischio mediante la stipula di specifiche assicurazioni o attraverso l'outsourcing.

L'analisi dei rischi fornisce quindi dati che possono dare precise indicazioni atte a stabilire le misure di sicurezza che devono essere adottate per garantire continuità dell'erogazione dei servizi.

12.9 Definizione del Piano di trattamento del rischio

Le attività previste all'interno di tale fase prevedono l'elaborazione di un report (Piano di Trattamento rif. Dato personale Inventory) volto ad evidenziare i valori di rischio rilevati per le categorie di dato personale ed a fornire le indicazioni atte a pianificare gli interventi e le contromisure di sicurezza necessarie alla riduzione dello stesso a livelli ritenuti accettabili per a società.
Tale piano comprende la definizione di attività e piani di miglioramento, che possono prevedere sia interventi di natura tecnico-operativa che di natura organizzativa. A completamento, devono essere definite anche le tempistiche per l'attuazione, nonché le responsabilità in termini di implementazione.
A fronte dell'applicazione del Piano di Trattamento, per ogni dato personale rimarrà associato un rischio residuo che tipicamente dovrà essere inferiore o uguale al rischio accettabile.
L'identificazione del valore di rischio accettabile consente di individuare le situazioni in cui il risultato del calcolo dà una valutazione di rischio sopra la soglia di accettabilità.
In questo caso opportune contromisure devono essere messe in atto per condurre il livello di rischio al di sotto della soglia accettabile.

Oltre alle contromisure da applicare, il Piano di Trattamento del Rischio definisce i tempi, i ruoli e le responsabilità relative all'implementazione delle stesse.
Le contromisure sono definite in base al loro stato di implementazione ed in relazione al loro peso complessivo nell'abbattimento del rischio.

12.10 Documenti di registrazione

L'output della valutazione è riportato nell' **Allegato 2 Analisi dei rischi**. La valutazione deve essere ripetuta ad intervalli regolari (generalmente ogni anno) e a fronte di qualsiasi variazione significativa relativa al dato personale e quindi all'Organizzazione.

13. NOTIFICA IN CASO DI DATA BREACH

Ai sensi dell'Articolo 33 del GDPR, ovvero in caso di violazione di archivi contenenti dati personali (ma, anche, in caso di smarrimento o furto di una chiavetta, di un hard disk esterno o di un computer portatile) l'azienda attiva la seguente procedura:

- Notifica la suddetta violazione all'autorità di controllo competente (ossia: al Garante) entro 72 ore dal momento in cui ne è venuto a conoscenza;
- Comunica a tutti gli utenti/interessati cui i dati si riferiscono, a meno che sia improbabile che quella violazione dell'archivio rappresenti un rischio per i diritti e le libertà delle persone fisiche.

Oltre il termine di 72 ore, tale comunicazione sarà accompagnata dalle ragioni del ritardo nell'agire in tal senso.
La notifica, in particolare, indicherà:

- La natura della violazione,
- Le categorie e il numero approssimativo dei dati personali violati e degli interessati coinvolti;
- Il nome e i dati di contatto del responsabile interno del trattamento dell'Azienda o di un altro punto di contatto presso cui sia consentito ottenere più informazioni;
- Le probabili conseguenze della violazione e le misure adottate, o di cui si propone l'adozione, al fine di porre rimedio alla violazione o di attenuarne i possibili effetti negativi.

14. NOMINA DPO DATA PROTECTION OFFICER – RPD RESPONSABILE DELLA PROTEZIONE DEI DATI

Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:
a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10

La **A.C.I. Promoter srl** non rientrando tra le fattispecie di cui sopra, non ha al momento nominato un DPO.

15. ALLEGATI

IO 01 - Policy aziendale per trattamenti elettronici e/o automatizzati
IO 02 - Policy aziendale per trattamenti con supporti cartacei
Allegato 1 Registro dei trattamenti
Allegato 2 Analisi dei rischi
Allegato 3 Informativa dipendenti
Allegato 3.1 Informativa lavoratori in distacco
Allegato 4 Informativa fornitori
Allegato 4.1 Informativa clienti
Allegato 5.1 Nomina responsabile del trattamento interno
Allegato 5.2 Nomina responsabile del trattamento esterno
Allegato 6 Atto di autorizzazione al trattamento dei dati