MANUALE OPERATIVO GDPR

General Data Protection Regulation

Redatto in base 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 alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

FIABA ETS

Sede legale: Piazzale degli Archivi, 41 – 00144
Roma
Titolare trattamento dati: Sig. Stefano Maiandi

Fiaba ETS si è costituita in data 27/07/2000 si è costituita FIABA con atto notarile (Studio Notarile – Dr. Antonio Mosca – n. repertorio 57.622 – n. 9678 di raccolta), con sede in Roma Piazzale degli Archivi n. 41 – 00144 Roma – C.F. 97240590584 presieduta da Giuseppe Trieste;
che con direttiva n° 96 del 28/02/03, la Presidenza del Consiglio dei Ministri, su proposta di FIABA, ha indetto la giornata nazionale di sensibilizzazione all'abbattimento delle barriere architettoniche (FIABADAY) che si terrà la prima domenica di ottobre di ogni anno;
che, FIABA ha già firmato protocolli d'intesa in tema di barriere culturali e fisiche con la Presidenza del Consiglio dei Ministri, con i Ministeri, le Regioni, le Province, i Comuni, le Università, gli Istituti di cultura e le associazioni di categoria;
che, FIABA si pone quale obiettivo primario l'abbattimento delle barriere culturali e fisiche che impediscono qualità di vita e pari opportunità per tutte le persone;
che, FIABA esplicita ed individua i diversi livelli di responsabilità e coinvolgimento di persone associazioni, ordini, enti, istituzioni ed aziende prendendo come modello di riferimento quello della "rete", in cui le relazioni tra gli attori pubblici e privati siano ispirate al principio della sussidiarietà e non più della delega e dell'assistenzialismo;
che, in questo nuovo quadro "politico-culturale", assume rilevanza particolare il ruolo che viene assegnato ai Ministeri, agli enti locali, agli operatori privati e alle associazioni per concorrere attivamente alla presa in carico e alla risoluzione della problematica;

DOCUMENTO REDATTO IN COLLABORAZIONE CON:

0	30/09/2022	PRIMA EMISSIONE	NAIKE S.r.l.	DIR
REV.	DATA	DESCRIZIONE REVISIONE	REDATTO	APPROVATO

SOMMARIO

1. DOCUMENTO

1.1 SCOPO

Il presente è redatto dall'azienda FIABA ETS. per soddisfare il REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 Aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
Inoltre costituisce un valido strumento per l' adozione delle misure idonee previste dallo stesso regolamento in accordo alla "responsabilizzazione" (accountability nell'accezione inglese) di titolari e responsabili, ossia, sull' adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento (si vedano artt. 23-25, in particolare, e l'intero Capo IV del regolamento). In sostanza rappresenta lo strumento affidato ai titolari per la definizione delle modalità, le garanzie e i limiti del trattamento dei dati personali nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

1.2 CAMPO DI APPLICAZIONE

Il Documento definisce le politiche e gli standard di sicurezza in merito al rischio inerente al trattamento dei dati adottati dall'azienda.
Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati (si vedano art . 75-77); tali impatti saranno analizzati attraverso un apposito processo di valutazione (si vedano artt. 35-36) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi. All'esito di questa valutazione di impatto il titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'Autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'art. 58: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.
Il presente documento e le relative informative in allegato si applicano:

- a tutti i lavoratori dipendenti e a tutti i collaboratori della FIABA ETS. a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratori a progetto, agenti, stagisti, consulenti, ecc.) che si trovano ad operare sui dati personali di cui la FIABA ETS. stessa è Titolare (di seguito "utenti");
- a tutte le attività o comportamenti comunque connessi all'utilizzo della rete Internet e della posta elettronica, mediante strumentazione aziendale o di terze parti autorizzate all'uso dell'infrastruttura aziendale.

1.3 RIFERIMENTI N O R M A T I V I

1. REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

2. Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679

1.4 Definizioni

1) «dato personale»: qualsiasi informazione riguardante una persona fisica o giuridica identificata o identificabile («interessato»); come il nome, la ragione sociale di un'azienda, un numero di identificazione, dati relativi all'ubicazione, un identificativo online (e-mail)e recapiti telefoni.
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;

Dati Considerati particolari (punto 13-14-15)

Art. 9 del GDPR, "Trattamento di categorie particolari di dati personali", dopo avere affermato il principio per cui "1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona", al comma 2 il Regolamento precisa alcune eccezioni a tale divieto, tra le quali – alla lettera e) – annovera il caso del trattamento che "riguarda dati personali resi manifestamente pubblici dall'interessato".
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 (1);

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.

2. PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI PERSONALI

I dati personali di FIABA ETS. 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»).

Le informazioni necessarie a definire i trattamenti sono richiamate nell'allegato 1 : Registro delle attività del trattamento

3. LICEITA' DEL TRATTAMENTO

I trattamenti di FIABA ETS. sono leciti in quanto ricorrono almeno una delle seguenti condizioni:
-l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità:

- 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;
- il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
- il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- 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;
- 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.

Il regolamento conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica; i fondamenti di liceità del trattamento sono indicati all'art. 6 del regolamento e coincidono, in linea di massima, con quelli previsti del Codice privacy - d.lgs. 196/2003 (consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati).

Le specifiche di liceità sono verificate nell'allegato 1 : Registro delle attività del trattamento

4. CONDIZIONI PER IL CONSENSO

FIABA ETS. basa le condizioni del consenso sui seguenti punti :

1 Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.
2.Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.
3.L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò.
Il consenso è revocato con la stessa facilità con cui è accordato.
4.Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

Le specifiche sul consenso relativamente ai vari trattamenti sono indicate nell'allegato 1:Registro delle attività del trattamento

5. TRATTAMENTO DI DATI PARTICOLARI

Premesso che il regolamento formalizza che é vietato trattare dati particolari che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, tale trattamento non si applica per FIABA ETS. in quanto l'azienda non tratta dati particolari o si verifica almeno uno dei seguenti casi:
a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati particolari per una o più finalità specifiche;
b)il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;
c)il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati particolari non siano comunicati all'esterno senza il consenso dell'interessato;

e) il trattamento riguarda dati particolari resi manifestamente pubblici dall'interessato;

f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;

g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;

h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità. In questo caso è il Medico competente dell'azienda che tratta i dati particolari dei dipendenti non direttamente l'azienda.

i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;

J) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Il trattamento di tali dati è indicato nell'allegato 1 : Registro delle attività del trattamento.

6. DIRITTI DELL'INTERESSATO

6.1 INFORMAZIONI DA FORNIRE QUALORA I DATI PERSONALI SIANO RACCOLTI PRESSO NL'INTERESSATO

FIABA ETS. in caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:

a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;
c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d) i legittimi interessi perseguiti dal titolare del trattamento o da terzi ove richiesto;
e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f)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, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.

In aggiunta alle informazioni di cui sopra, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:

a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
b) 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;
c) l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
d) il diritto di proporre reclamo a un'autorità di controllo;
e) 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;
f) 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.

6.2 INFORMAZIONI DA FORNIRE QUALORA I DATI PERSONALI NON SIANO STATI OTTENUTI PRESSO L'INTERESSATO

Qualora i dati non siano stati ottenuti presso l'interessato, il titolare del trattamento fornisce all'interessato le seguenti informazioni:

a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;
c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d) le categorie di dati personali in questione;
e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un destinatario in un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.

Oltre alle informazioni di cui sopra il titolare del trattamento dei dati di FIABA ETS. fornisce all'interessato le seguenti informazioni necessarie per garantire un trattamento corretto e trasparente nei confronti dell'interessato:

a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
c) 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 dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
d) qualora il trattamento sia relativo a dati particolari l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca;
e) il diritto di proporre reclamo a un'autorità di controllo;
f) la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;
g) 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.

Il titolare del trattamento fornisce le informazioni di cui sopra

a) entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;
b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato;

c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.

Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati ottenuti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni informazione pertinente, non fornisce informativa nella misura in cui l'interessato dispone già delle informazioni e negli altri casi provvede a dare informativa relativa a quanto sopra con ausilio di Informative (allegato 5-6)

6.3 Diritto di accesso dell'interessato, diritto di rettifica, diritto alla cancellazione (diritto all'oblio), diritto di limitazione di trattamento, obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento, diritto di portabilità dei dati e diritto di opposizione (art 16-21 del Regolamento GDPR 679/2016)

In relazione a quanto sopra l'interessato di FIABA ETS. ha diritto di accesso, diritto di rettifica, diritto alla cancellazione ed eventuale diritto di limitazione di trattamento, ovvero diritto di portabilità dei dati e diritto all'oblio.

L'interessato ha il 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 alle seguenti informazioni:

a) le finalità del trattamento;
b) le categorie di dati personali in questione;
c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
f) il diritto di proporre reclamo a un'autorità di controllo;
g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
h) 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.

Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate relative al trasferimento.

Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la

richiesta mediante mezzi elettronici e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa

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 e se non sussiste altro fondamento giuridico per il trattamento;

c) l'interessato si oppone al trattamento , e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento

d) i dati personali sono stati trattati illecitamente;

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 , in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato.

Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

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 compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto. Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità.

7. RUOLI, COMPITI DELLE FIGURE PREVISTE PER LA SICUREZZA DEI DATI PERSONALI

7.1 TITOLARE DEL TRATTAMENTO

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, il titolare del trattamento di FIABA ETS. mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente documento . Dette misure sono riesaminate e aggiornate qualora necessario ed includono l'attuazione di politiche adeguate in materia di protezione dei dati.

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento di FIABA ETS. mette in atto misure tecniche e organizzative adeguate, volte ad attuare in modo efficace i principi di protezione dei dati e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

Il titolare del trattamento dati di FIABA ETS. mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Il Titolare del trattamento dei dati è il Sig. Stefano Maiandi .

7.2 RESPONSABILE DEL TRATTAMENTO

Qualora un trattamento debba essere effettuato per conto del titolare del trattamento di FIABA ETS., quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento.

Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto (delega) che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

Il contratto (delega) prevede, in particolare, che il responsabile del trattamento:

a) tratti 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 informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

c) adotti tutte le misure richieste

d) rispetti le condizioni previste per ricorrere a un altro responsabile del trattamento;

e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in 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 ;

f) assista il titolare del trattamento nel garantire il rispetto degli obblighi sicurezza e consultazione preventiva , tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti;

h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato

Il Responsabile del trattamento dei dati è Raffaella Bianchi.

Si rimanda alla Allegato 2: Nomina del responsabile del trattamento dei dati personali

8. REGISTRI DELLE ATTIVITÀ DI TRATTAMENTO

Il titolare del trattamento ed ogni responsabile o gli incaricati tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte 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 DPO se necessario.
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
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 Si rimanda ai registri riportati nell'allegato 1 : Registro delle attività del trattamento

9. SICUREZZA DEL TRATTAMENTO

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento di
FIABA ETS. ed i responsabili del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
a) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
b) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
c) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
Nel valutare l'adeguato livello di sicurezza, il titolare del trattamento dei dati ed i responsabili del trattamento tengono conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
Le misure di sicurezza dei trattamenti sono riportate nell'allegato 1 : Registro delle attività del trattamento.

10. NOTIFICA DI UNA VIOLAZIONE DEI DATI PERSONALI ALL'AUTORITÀ DI CONTROLLO E COMUNICAZIONE DI UNA VIOLAZIONE DEI DATI PERSONALI ALL'INTERESSATO

In caso di grave violazione dei dati personali, il titolare del trattamento dati, notifica la violazione all'autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione. La notifica contiene :

a)descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) descrizione delle probabili conseguenze della violazione dei dati personali;

d) descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Il titolare del trattamento dati, documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio in apposito registro Data Breach . Tale documentazione consente all'autorità di controllo di verificare il rispetto del REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016

Si rimanda al registro Data Breach(allegato 9) ed al Modello segnalazione Data Breach(allegato 10).

Non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati

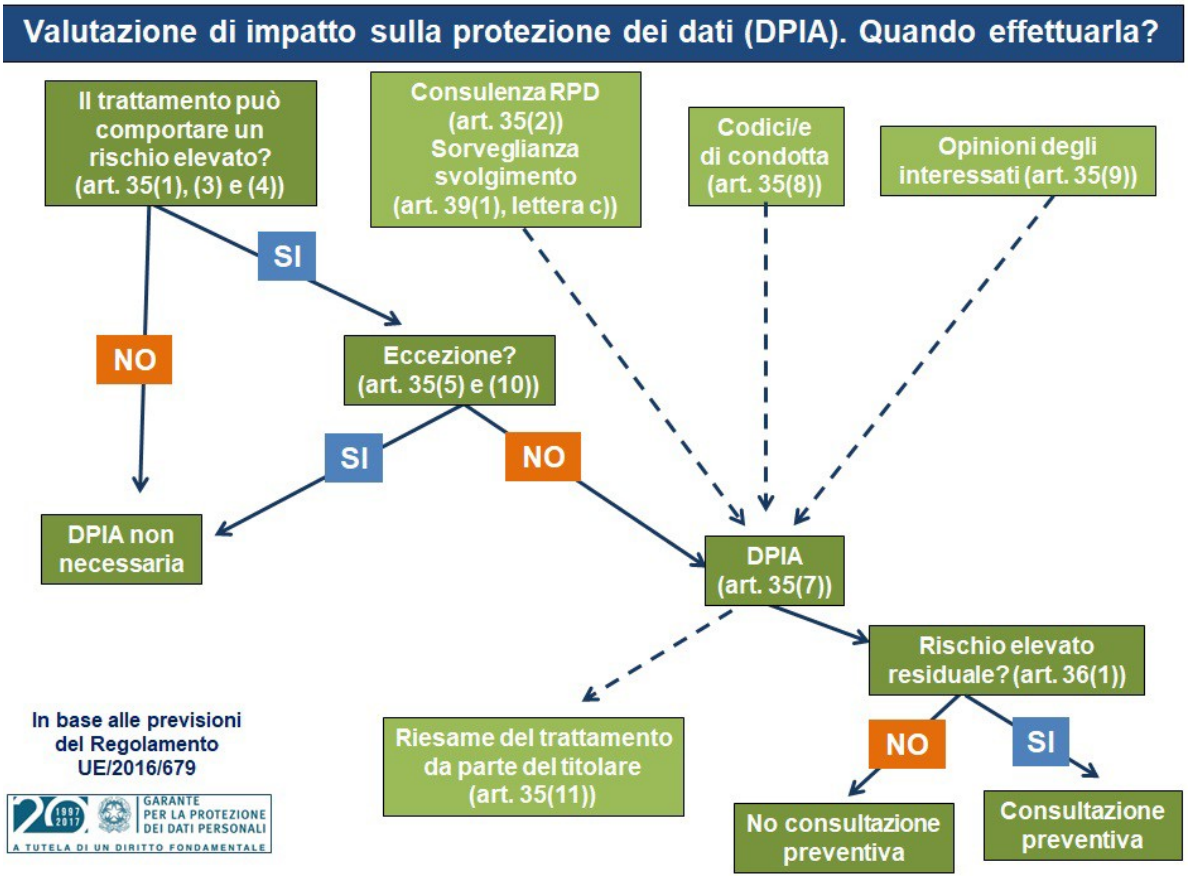
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

11. VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento deve effettuare, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.
La valutazione d'impatto sulla protezione è richiesta in particolare nei casi seguenti:
a)una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
b) il trattamento, su larga scala, di categorie dati particolari.
c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.
L'Azienda anche se non rientra nelle casistiche sopracitate, ha provveduto redigere una valutazione dei rischi con il metodo sotto riportato.

La valutazione contiene
a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati
d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.
Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati

Il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto nell'ambito della valutazione.
Il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.



FIABA ETS ha identificato tutti i rischi aziendali analizzando i propri trattamenti e suddividendo in rischi in:

- Rischi nei confronti degli individui (es. rischi per la sicurezza fisica, rischi materiali (es. perdite finanziarie causate da frodi o dati inesatti i violazione della sicurezza) e rischi morali (es. preoccupazione per la diffusione di una notizia riservata o per un'intrusione non prevista)
- Rischi nei confronti dell'organizzazione possono consistere in danni alla reputazione con conseguente perdita di business o in costi finanziari dovuti alla una violazione di dati ;

- □ Rischi di conformità (es. al GDPR, alle indicazioni del garante,) possono comportare multe o penali

FIABA ETS. ha quindi effettuato tale analisi dei rischi per i trattamenti riportati in Allegato 1, Si riserva comunque in futuro di ampliare l'analisi ad altri trattamenti che dovessero essere implementati in azienda.
Con questa fase sono identificati i rischi potenziali nei quali FIABA ETS. potrebbe incorrere.

Un metodo semplice ed efficace per poter effettuare la stima/analisi del rischio e definirne l'accettabilità o meno, può essere la matrice, in cui le due variabili, gravità dell'impatto (G) e la probabilità (P) e la Proporzionalità delle misure (I); ciascun parametro viene categorizzato (in 4 livelli), ottenendo così un prodotto dei tre parametri che riassume il livello di rischio di ogni situazione individuata.
Il prodotto delle variabili
R = G*P*I quantificherà la stima del rischio.
Di seguito riportiamo le tabelle dei tre parametri:

Tabella delle probabilità di accadimento dell'evento (P)

Criteri	Livello	Valore
L'evento rilevato può provocare un Impatto per la concomitanza di più eventi poco probabili e indipendenti fra loro. Non sono noti episodi già verificatisi.	Improbabile	1
L'Evento rilevato può provocare un Impatto solo in circostanze sfortunate di eventi. Sono noti solo rarissimi episodi già verificatisi negli ultimi 5 anni	Poco Probabile	2
L'Evento rilevato può provocare un Impatto anche se non in modo automatico o diretto. E' noto qualche episodio già verificatosi negli ultimi 5 anni	Probabile	3
Esiste una correlazione diretta tra evento ed il verificarsi dell'Impatto ipotizzato. Si sono già verificati danni per lo stesso pericolo rilevato negli ultimi 5 anni.	Altamente Probabile	4

Tabella Gravità (G)

Criteri	Livello	Valore
L'impatto risulta pressoché irrilevante	Lieve	1
L'impatto comporta una perdita contenuta	Medio	2
L'impatto comporta una perdita significativa	Grave	3
L'impatto comporta una perdita con gravi effetti sulla stabilità economico finanziaria aziendale e sulle libertà e i diritti degli interessati	Gravissimo	4

Tabella necessità e proporzionalità (I)

Criteri	Livello	Valore
Le misure intraprese sono coerenti e proporzionali e secondo necessità rispetto al trattamento oggetto	Conformi	1
Le misure intraprese sono lievemente superiori/inferiori e comunque sproporzionate e quindi oltremodo necessità rispetto al trattamento oggetto	Non proporzionate	2
Le misure intraprese sono inferiori, comunque non proporzionali ed insufficienti rispetto alla necessità del l trattamento oggetto	Inferiori	3

Classificazione dei livelli di rischio

Il processo di valutazione che porta ad associare ad uno scenario talvolta complesso, un giudizio espresso in forma numerica, risente ovviamente di tutta una serie di incertezze ed approssimazioni. La molteplicità dei fattori che concorrono a definire una condizione di rischio, porta necessariamente a categorizzare le variabili del problema e a risentire delle incertezze nella definizione delle stesse.
Per tale motivo, il livello di rischio calcolato come di seguito serve ad individuare una classe di rischio per ogni situazione analizzata

R = G*P *I

Il giudizio espresso quindi in forma lessicale è categorizzato in tre livelli a seconda dell'importanza del rischio stesso.

Stima del rischio (R_K = P x I)		
R x 8	8 x R x 24	R □ 24
Rischio BASSO (B)	Rischio MEDIO (M)	Rischio ALTO (A)
Area Accettabile	Area medio	Area Inaccettabile

Area Rischio basso (accettabile)

In questo caso il rischio è così basso da essere trascurabile e non deve essere necessariamente perseguito il controllo del rischio o attivate azioni correttive.

Area Rischio medio

All'interno di quest'area l'azienda si prodiga per ridurre per quanto possibile i rischi, ponderandone il rischio residuo e la praticabilità di un'ulteriore riduzione, tramite:

- la praticabilità tecnica;
- la praticabilità economica.

La praticabilità tecnica ed organizzativa si riferisce alla capacità di ridurre il rischio con misure tecniche ed organizzative , indipendentemente dal costo.
La praticabilità economica fa riferimento alla capacità di ridurre il rischio senza rendere l'intervento economicamente inaccettabile, considerato lo stato dell'area generalmente accettata. Vicino all'area accettabile, si ritiene sufficiente il rapporto rischi/benefici.

Le azioni, se ritenute necessarie, andranno inserite all'interno del piano di miglioramento o nella modulistica delle azioni correttive/preventive.

Area Rischio alto (inaccettabile)

Il rischio è così alto da non poter essere tollerabile, e dev'essere perseguito il suo controllo per una sua eliminazione o riduzione a livelli accettabili. Sono quindi prescritte azioni correttive o di miglioramento a breve termine.
Le azioni andranno inserite all'interno del piano di miglioramento e documentate

Valutazione

Se il risultato dell'analisi ricade nell'area di accettabilità, verrà definito un obiettivo per renderlo tale.

Azioni

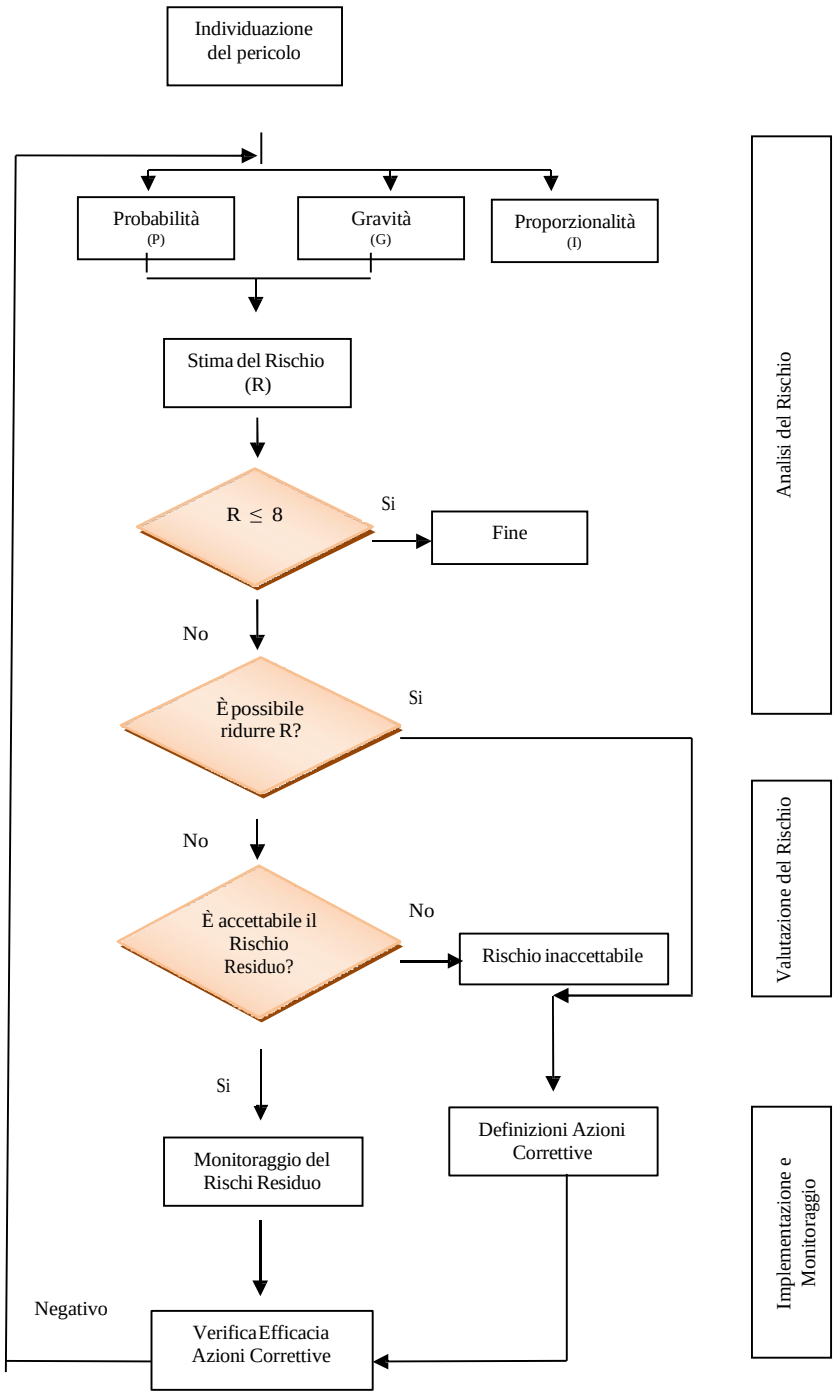
È costituito dalle fasi:

- predisposizione delle azioni correttive (interventi migliorativi);
- monitoraggio del rischio residuo.

Le azioni correttive saranno rivolte, ove possibile, all'eliminazione del pericolo, ovvero alla riduzione del rischio fino ad un livello accettabile, tenuto sempre presente la praticabilità tecnica ed economica.
I tempi di attuazione delle azioni correttive saranno individuati in base al livello di rischio stimato in:

LIVELLO DI RISCHIO	TEMPI DI ATTUAZIONE DELLE AZIONI CORRETTIVE (misure di sicurezza)
Rischio alto (A)	Azioni correttive/piano di miglioramento immediate o da programmare con urgenza
Rischio medio (M)	Eventuali Azioni correttive-preventive/piano di miglioramento da valutare o da programmare nel breve –medio periodo
Rischio basso (B)	Non è richiesta alcuna azione

Diagramma di flusso del processo di Valutazione del Rischio



Sulle risultanze dei singoli fattori di rischio valutati, si individuano le misure correttive ritenute necessariamente immediate o programmabili.

Gli impatti sono valutati secondo le seguenti cause riportate nell'Allegato 3 Analisi cause:
-Incendio
-Acqua,
-Incidente
-Cedimento strutturale
-Fenomeni metereologici
-Fenomeni sismici
-Alluvioni ed allagamenti
-Guasti generali
- Malfunzionamenti
- Radiazioni
-Violazioni privacy
- Guasti tecnici
- Abuso di diritti
- Errori umani
- Dipendenza dell'azienda
- Danneggiamento accidentale
- Accesso accidentale

Si rimanda all'allegato 4 : Valutazione impatto protezione dati

12. DPO DATA PROTECTION OFFICER

E' obbligatorio nominare il DPO nei seguenti casi:

- Amministrazione e enti pubblici fatte eccezione per autorità giudiziaria;
- Soggetti la cui attività principale consiste in trattamenti che, per la loro natura e il loro oggetto o le loro finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
- Soggetti la cui attività principale consiste nel trattamento, su larga scala, di dati Particolari, relativi alla saluta o alla vita sessuale genetici, giudiziari e biometrici.

Il DPO è Responsabile della Protezione dei Dati e deve:

- Possedere una adeguata conoscenza della normativa e della prassi di gestione dei dati Personali:
- Adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse;
- Operare sulla Base di un contratto; Il

DPO deve eseguire i seguenti compiti:

- Sorvegliare l'osservanza del regolamento;
- Supportare il titolare in ogni attività connessa al trattamento dei dati Personali anche con riguardo alla tenuta di un registro dell'Attività di Trattamento;
- Supportare nella valutazione d'impatto sulla protezione dei Dati:

- Informare e sensibilizzare il Titolare o il Responsabile nonché i dipendenti riguardo agli obblighi del Regolamento;
- Cooperare con le autorità di controllo e fungere da punto di contatto;

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; oppure

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

Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti .

Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi.

Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo.

Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

Il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei suoi compiti fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.

Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.

Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.

Il responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti.

Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi

Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del

trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento
d) cooperare con l'autorità di controllo; e
e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva.
Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo

L'azienda FIABA ETS. non rientra tra i casi sopramenzionati, di conseguenza non ha provveduto a nominare un responsabile di protezione dei dati, DPO.

.13. RESPONSABILE DEL TRATTAMENTO DEI DATI

L'azienda anche se non rientra nell'obbligo di nominare un DPO deve nominare un Titolare del Trattamento dei dati che a suo volta può nominare un Responsabile del trattamenti dati. Titolare del trattamento è la Direzione Aziendale o l'Amministratore.
Responsabile del trattamento la persona fisica o giuridica che tratta i dati personali per conto del Titolare del trattamento.
Il Responsabile del Trattamento può nominare a sua volta degli incaricati per il trattamento dei dati.
In Allegato 12 organigramma funzionale per il Trattamento dei dati.

14. PIANO DI FORMAZIONE DEL PERSONALE AUTORIZZATO AL TRATTAMENTO DEI DATI

Al "Titolare del trattamento" è affidato il compito di verificare ogni anno, entro il 31 dicembre, le necessità di formazione del personale "Incaricato del trattamento" dei dati con lo scopo di fornire ogni informazione necessaria a migliorare la sicurezza di trattamento dei dati.
Per ogni utente il "Titolare del trattamento " definisce, sulla base dell'esperienza e delle sue conoscenze, ed in funzione anche di eventuali variazioni della normativa, le necessità di formazione, i vari partecipanti alle formazioni saranno registrati nell'apposito Allegato 11 Piano di formazione.

15. MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

15.1 SISTEMA DI AUTENTIFICAZIONE INFORMATICA, PASSWORD INTERNE AZIENDALI

L'azienda adotta istruzioni per mantenere una sicurezza tecnica sulle password dei pc aziendali, ovvero:

- la credenziale di autenticazione ricevuta per il trattamento dei dati deve essere memorizzata con segretezza ed ad uso esclusivo;
- la parola chiave, prevista dal sistema di autenticazione, deve essere composta da otto caratteri; non deve contenere riferimenti riconducibili a persone fisiche; deve essere modificata ogni 6 mesi;
- usare sia lettere che numeri e almeno un carattere maiuscolo;
- non basare la scelta su informazioni facilmente deducibili quali, ad esempio, il proprio nome, il nome dei
- propri familiari, le date di nascita, i codici fiscali, ecc.,
- mantenerla riservata e non divulgarla a terzi;
- non permettere ad altri utenti di operare con il proprio identificativo utente;
- non trascriverla su supporti (es. fogli, post-it) facilmente accessibili a terzi, né lasciarla memorizzata sul proprio PC;
- non comunicarla mai per telefono salvo gravi necessità.
- non è consentito lasciare incustodito o accessibile l'elaboratore durante la sessione di trattamento dei dati; per evitare l'accesso non autorizzato alle banche dati elettroniche, l'elaboratore utilizzato è impostato prevedendo in automatico il blocco del sistema (richiesta reinserimento password);
- si deve controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti ed i documenti cartacei prelevati dagli archivi; al termine dell'utilizzo si è tenuti a riporre quanto prelevato nel luogo preposto alla conservazione; per le norme generali di prevenzioni, possibilmente in armadi chiusi a chiave.
- Ad ogni "Incaricato del Trattamento" è stata assegnata una credenziale per l'autentificazione.
- Non sono ammessi nomi identificativi di gruppo.
- La parola chiave è individuale, disattivata in caso di perdita o dimissioni dell'"Incaricato del Trattamento" durante la digitazione non può comparire in chiaro sul monitor e non può rimanere nella memoria del computer
- Le password di tutti i pc e server sono custodite dal Responsabile trattamento dati, all'interno di foglio excel protetto da password oppure sopra un foglio cartaceo chiuso all'interno di armadio con serratura.

  L'azienda FIABA ETS. ha installato su tutti i pc un software di crittografia dei dati e la visualizzazione di alcune cartelle come quella della contabilità e scansione documenti della contabilità è limitata solo ad alcuni utenti.

15.2 ACCESSO AI DATI DALLA POSTAZIONE DI LAVORO

La postazione di lavoro deve essere:

- utilizzata solo per scopi legati alla propria attività lavorativa;
- utilizzata in modo esclusivo da un solo utente;
- protetta, evitando che terzi possano accedere ai dati che si sta trattando

Occorre, inoltre, precisare che è dovere dell'Incaricato:

- non utilizzare in Azienda risorse informatiche private (PC, periferiche, token, ecc..);
- non installare alcun software;
- non lasciare sulla scrivania informazioni riservate su qualunque supporto esse siano archiviate (carta, chiavette USB ecc.)
- richiamare le funzioni di sicurezza del sistema operativo (con la sequenza dei tasti CTRL+ALT+CANC) ed assicurarsi della attivazione della funzione Lock Workstation in caso di abbandono momentaneo del proprio PC o, in alternativa, impostare lo screen saver con password in modo che si attivi dopo max.5 minuti di inattività;
- non lasciare il computer portatile incustodito sul posto di lavoro (al termine dell'orario lavorativo, durante le pause di lavoro, o durante riunioni lontane dalla propria postazione);
- non lasciare incustoditi cellulari e palmari;
- non utilizzare fax e/o telefono per trasmettere informazioni riservate e personali se non si è assolutamente certi dell'identità dell'interlocutore o del destinatario e se esso non è legittimato a riceverle.

15.3 PROTEZIONE DEI PC PORTATILI

Un computer portatile presenta maggiori vulnerabilità rispetto ad una postazione di lavoro fissa. Fatte salve tutte le disposizioni dei paragrafi precedenti, di seguito vengono illustrate le ulteriori precauzioni da adottare nell'uso dei dispositivi portatili:

- conservare lo strumento in un luogo sicuro alla fine della giornata lavorativa;
- non lasciare mai incustodito l'elaboratore in caso di utilizzo in ambito esterno all'azienda;
- avvertire tempestivamente l'Area IT, che darà le opportune indicazioni, in caso di furto di un PC portatile;
- essere sempre ben consapevole delle informazioni archiviate sul portatile il quale è maggiormente soggetto a furto e smarrimento rispetto alla postazione fissa;
- operare sempre nella massima riservatezza quando si utilizza il PC portatile in pubblico: i dati, ed in particolare le password, potrebbero essere intercettati da osservatori indiscreti.

15.4 BACK UP

Il back up è la replicazione su un qualunque supporto di memorizzazione di materiale informativo archiviato nella memoria di massa dei computer, siano essi personal computer, workstation o server, home computer o smartphone, al fine di prevenire la perdita definitiva dei dati in caso di eventi malevoli accidentali o intenzionali. Si tratta dunque di una misura di ridondanza fisica dei dati.
Un secondo scopo è quello di recuperare i dati da un momento precedente, cioè utilizzare una versione precedente rispetto a quella attuale, di dati attualmente in possesso, secondo una politica di conservazione dei dati definiti dall'utente, tipicamente configurata all'interno di un software di backup.
Un backup può essere fatto in diverse modalità, su degli appropriati hard disk esterni, chiamati per l'appunto NAS, su uno o più banali supporti ottici come CD, DVD e/o Blu-Ray, su delle semplici pen drive USB, su delle pratiche microSD, e in generale, su un qualunque altro valido supporto di memorizzazione. Una copia di backup, può anche essere fatta direttamente sul cloud, one drive ecc.
Fino a quando i nuovi dati vengono creati e modificati, sarà sempre necessario eseguire backup con un certa frequenza. Gli individui e le organizzazioni, partendo da un computer fino a migliaia di sistemi informatici hanno tutti la necessita di proteggere i dati. Le scale possono essere molto diverse, ma gli obiettivi e limitazioni sono essenzialmente le stesse. Chi gestisce il processo di backup è quindi tenuto a valutare e applicare le misure necessarie a garantire un certo grado di successo per la copia dei dati.

Obiettivi

Recovery Point Objective (RPO)

Essenzialmente è il momento in cui si effettua l'ultimo backup prima di un disastro. Il RPO desiderabile sarebbe il punto appena prima dell'evento di perdita dei dati poiché tutte le modifiche effettuate ai dati in istanti di tempo successivi a questo evento vengono perse. Si cerca quindi di realizzare operazioni di backup il più frequente possibile in modo da perdere il minor numero di dati possibile.

Recovery Time Objective (RTO)

La quantità di tempo trascorso tra il disastro e il ripristino delle funzioni aziendali, ovviamente dipende dal tipo di disastro e dalla bontà del piano di disaster recovery.

Sicurezza dei dati

Oltre a preservare l'accesso ai dati per i suoi proprietari, bisogna mettere in pratica misure che riescano ad impedire accessi non autorizzati, per esempio tramite crittografia dei dati e politiche di gestione dei supporti adeguati.

Periodo di conservazione dei dati

Regolamenti e la politica di gestione del backup possono portare a situazioni in cui si prevede che le copie devono essere conservate per un periodo particolare, ma non oltre. Mantenere il backup dopo questo periodo può portare a responsabilità indesiderate e l'uso non ottimale dei supporti di memorizzazione.

All'interno della sede legale di FIABA ETS. il back-up avviene all'interno di due server fisici in azienda posizionati in una stanza dedicata con climatizzatore e dispositivo di rilevazione fumo e temperatura.
Sono presenti anche 4 NAS di archivio per i file di posta, l'archiviazione della posta avviene sopra sopra1 NAS con 4 dischi e in più viene replicato sopra un NAS uguale identico.
Viene utilizzato 1 NAS per i documenti Autocad e 1 per la replica.
Per effettuare le repliche si utilizzano 2 NAS esterni dove ogni venerdì si attaccano al server e partono in automatico. Il lunedì vengono portati esternamente all'azienda.
Sono presenti anche 4 server virtuali dedicati(server di dominio, server per la posta elettronica Exchange, uno per i documenti word e cad e un server virtuale per il software gestionale).

15.5 PROTEZIONE DA VIRUS INFORMATICI

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita di dati a causa di Virus Informatici, il "Titolare del trattamento", stabilisce quali protezioni software adottare in relazione all'evoluzione tecnologica dei sistemi disponibili sul mercato.
Il "Titolare del trattamento", stabilisce inoltre la periodicità, con cui debbono essere effettuati gli aggiornamenti dei sistemi Antivirus utilizzati per ottenere un accettabile standard di sicurezza delle "Banche di dati" trattate

Il "Titolare del trattamento", nel caso in cui su uno o più sistemi si dovesse verificare perdita di informazioni o danni a causa di infezione o contagio da Virus Informatici deve inoltre provvedere a:

- Isolare il sistema.
- Verificare se ci sono altri sistemi infettati con lo stesso Virus Informatico.
- Identificare l'Antivirus adatto e bonificare il sistema infetto.
- Installare l'Antivirus adatto su tutti gli altri sistemi che ne sono sprovvisti.

L'azienda utilizza antivirus centralizzato nel server che si aggiorna automaticamente su ogni postazione ed è impostato un firewall di rete, gli ospiti non possono entrare nella rete aziendale ma possono viaggiare su una rete separata.

15.6 MISURE DI SICUREZZA CONTRO IL RISCHIO DI ACCESSO NON AUTORIZZATO E TRATTAMENTO NON CONSENTITO

NORME GENERALI DI PREVENZIONE

È fatto divieto a chiunque di:

- Effettuare copie su supporti magnetici o trasmissioni non autorizzate dal "Titolare del trattamento" di dati oggetto del trattamento.
- Effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal "Titolare del trattamento" , di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.
- Sottrarre, cancellare, distruggere senza l'autorizzazione del "Titolare del trattamento", stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.
- Consegnare a persone non autorizzate dal "Titolare del trattamento", stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

15.7 PROCEDURE PER CONTROLLARE L'ACCESSO AI LOCALI IN CUI VENGONO TRATTATI I DATI

Al "Titolare del trattamento "è affidato il compito impartire idonee istruzioni al fine di:

- Definire le modalità di accesso agli uffici in cui sono presenti sistemi o apparecchiature di accesso ai dati trattati.
- Impedire l'intrusione nei locali, da parte di persone non autorizzate.
- Impedire il danneggiamento, la manomissione, la sottrazione o la copia di dati.
- Conservare i documenti contenenti i dati in contenitori o locali muniti di serratura.

L'accesso ai locali aziendali non è consentito fuori dagli orari di chiusura, ad eccezione del personale autorizzato (rif. Lettere di incarico).
Gli uffici vengono sempre chiusi a chiave e i pc hanno tutti gli screen sever con le relative password.

15.8 PIANO DI VERIFICA DELLE MISURE ADOTTATE

La bontà delle misure adottate deve essere periodicamente verificata. Nello specifico le operazioni di verifica riguardano i seguenti:

- controllo e manutenzione degli estintori: effettuato da personale competente
- corretto utilizzo delle credenziali di autenticazione e disattivazione delle password scadute:
- aggiornamento antivirus periodico
- aggiornamento del livello di formazione degli incaricati: annualmente e in relazione dell'evoluzione tecnologica e teorica avvenuta in azienda

15.9 MANUTENZIONE DELLE APPARECCHIATURE E DEI SISTEMI DI TRATTAMENTO DEI DATI

Nel caso in cui esistano rischi evidenti ogni "Incaricato del trattamento" è tenuto ad informarne il "Titolare del trattamento", perché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

Al "Titolare del trattamento" è affidato il compito impartire adeguate istruzioni al fine di adottare il ripristino dell'apparecchiatura, tenendo conto anche dell'evoluzione tecnologica.

La manutenzione straordinaria dei sistemi di elaborazione è affidata a professionisti esterni, i quali hanno autorizzazione all'accesso alla banca dati informatica, al fine di operare il ripristino delle apparecchiature danneggiate / procedere all'aggiornamento dei sistemi informatici.

FIABA ETS. ha stipulato un contratto con una software house che si collega principalmente con TeamViewer, l'accesso in remoto è regolarizzato attraverso il contratto e l'allegato 7 Informativa per software house.

15.10 USO DI INTERNET E GESTIONE POSTA ELETTRONICA

Gli strumenti di comunicazione telematica (Internet e Posta elettronica) devono essere utilizzati solo ed esclusivamente per finalità lavorative. Sono vietati comportamenti che possano arrecare danno all'Azienda.

In particolare, l'utente dovrà osservare le seguenti regole:

- è consentita la navigazione internet solo in siti attinenti e necessari per lo svolgimento delle mansioni assegnate;
- non è consentito scaricare software gratuiti (freeware o shareware) prelevati da siti Internet;
- non è consentita la registrazione a siti internet o partecipare a Forum di discussione se questo non è strettamente necessario per lo svolgimento della propria attività lavorativa;
- non è consentito l'utilizzo funzioni di instant messaging a meno che autorizzate dall' Area IT;
- è vietato aprire e-mail e file allegati di origine sconosciuta o che presentino degli aspetti anomali (quali ad esempio, un soggetto non chiaro);
- non è consentito rispondere a messaggi provenienti da un mittente sconosciuto o di dubbio contenuto in quanto tale atto assicura al mittente l'esistenza del destinatario;
- è vietato l'utilizzo della posta elettronica per comunicare informazioni riservate, dati personali o dati critici, senza garantirne l'opportuna protezione;
- occorre sempre accertarsi che i destinatari della corrispondenza per posta elettronica siano autorizzati ad entrare in possesso dei dati che ci si appresta ad inviare;

- occorre sempre essere consapevoli che posta elettronica e navigazione Internet sono veicoli per l'introduzione sulla propria macchina (e quindi in azienda) di virus e altri elementi potenzialmente dannosi;
- è consentito solo l'utilizzo dei programmi ufficialmente installati dall'Area IT/ tecnico informatico/software house;
- è vietato installare autonomamente programmi, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti, di violare la legge sul diritto d'autore non disponendo delle apposite licenze d'uso acquistate dall'Azienda;
- è vietato modificare le caratteristiche impostate sulle dotazioni od installare dispositivi di memorizzazione, comunicazione o altro (ad esempio masterizzatori, modem, wi-fi o connect card),collegare alla rete aziendale qualsiasi apparecchiatura (ad es. switch, hub, apparati di memorizzazione di rete, ecc), effettuare collegamenti verso l'esterno di qualsiasi tipo (ad es. tramite modem o connect card ecc.) utilizzando un pc che sia contemporaneamente collegato alla rete aziendale (creando così un collegamento tra la rete aziendale interna e la rete esterna); al fine di ottimizzare le risorse a disposizione della posta elettronica aziendale e migliorare le prestazioni del sistema si evidenzia che la casella di posta deve essere "tenuta in ordine" cancellando periodicamente o comunque se sono superati i limiti di spazio concessi, documenti inutili o allegati ingombranti.
- va sempre prestata la massima attenzione nell'utilizzo dei supporti di origine esterna (per es. chiavi USB, dischi esterni ecc.), avvertendo immediatamente l'Amministratore di sistema nel caso in cui siano rilevati virus.
- L'utente, in caso di assenza programmata (ad esempio per ferie o attività di lavoro fuori sede) - di almeno 5 giornate lavorative - deve attivare l'apposita funzionalità di sistema (cd. "Fuori Sede") che consente di inviare automaticamente ai mittenti un messaggio di risposta contenente le "coordinate" (anche elettroniche o telefoniche) di un altro utente o altre modalità utili di contatto della struttura.
- L'azienda, in caso di assenza improvvisa o prolungata dell'utente o comunque non programmata e per improrogabili necessità di sicurezza o di operatività del sistema, si riserva, per mezzo dell'Amministratore di Sistema e Responsabile sistemi ICT, di accedere alla casella

di posta elettronica dell'utente assente: per i dettagli si rimanda al paragrafo 5 "Accesso ai dati dell'utente".

Particolari cautele nella predisposizione dei messaggi di posta elettronica.

Nell'utilizzo della posta elettronica ciascun utente deve tenere in debito conto che i soggetti esterni possono attribuire carattere istituzionale alla corrispondenza ricevuta da dipendenti aziendali. Pertanto si deve prestare particolare attenzione agli eventuali impegni contrattuali e precontrattuali contenuti nei messaggi.

La formulazione dei messaggi deve pertanto far uso di un linguaggio appropriato, corretto e rispettoso che tuteli la dignità delle persone, l'immagine e la reputazione dell'Azienda.

L'Azienda formula inoltre le seguenti regole di comportamento a cui gli utenti devono attenersi:

a) conservare le comunicazioni inviate o ricevute, in particolare quelle dalle quali si possano desumere impegni e/o indicazioni operative provenienti dalla Committenza pubblica;

b) prestare attenzione ai messaggi di posta elettronica ed ai file, programmi e oggetti allegati, ricevuti da mittenti sconosciuti, con testo del messaggio non comprensibile o comunque avulso dal proprio contesto lavorativo. In tali casi gli utenti devono in particolare:

- visualizzare preventivamente il contenuto tramite utilizzo della funzione "Riquadro di lettura" (o preview) e, nel caso si riscontri un contenuto sospetto, non aprire il messaggio,
- una volta aperto il messaggio, evitare di aprire gli allegati o cliccare sui "link" eventualmente presenti,
- cancellare il messaggio e svuotare il "cestino" della posta,
- segnalare l'accaduto all'Amministratore di Sistema

c) evitare di cliccare sui collegamenti ipertestuali dubbi presenti nei messaggi di posta: in caso di necessità, accedere ai siti segnalati digitando il nome del sito da visitare direttamente nella barra degli indirizzi nei consueti strumenti di navigazione;

d) in caso di iscrizione a servizi informativi accessibili via internet ovvero a servizi di editoria on line, veicolati attraverso lo strumento di posta elettronica :

- adoperare estrema cautela ed essere selettivi nella scelta della società che fornisce il servizio; in particolare l'adesione dovrà avvenire in funzione dell'attinenza del servizio con la propria attività lavorativa,

- utilizzare il servizio solo per acquisire informazioni inerenti finalità aziendali, facendo attenzione alle informazioni fornite a terzi in modo da prevenire attacchi di social engineering,
- in caso di appesantimento dovuto ad un eccessivo traffico di messaggi scambiati attraverso la lista di distribuzione, revocare l'adesione alla stessa. Si raccomanda, in proposito, di approfondire al momento dell'iscrizione le modalità per richiederne la revoca.

e) in caso di errore nella spedizione o ricezione, contattare rispettivamente il destinatario cui è stata trasmessa per errore la comunicazione o il mittente che, per errore, l'ha spedita, eliminando quanto ricevuto (compresi allegati) senza effettuare copia;

f) evitare di predisporre messaggi che contengano materiali che violino la legge sul diritto d'autore, o altri diritti di proprietà intellettuale o industriale.

15.11 TRASMISSIONE E RIPRODUZIONE DEI DOCUMENTI

Al fine di prevenire eventuali accessi ai dati aziendali da parte di soggetti terzi non autorizzati, occorre adottare delle cautele nella trasmissione e riproduzione dei documenti contenenti dati personali.

Quando le informazioni devono essere trasmesse telefonicamente occorre essere assolutamente certi dell'identità dell'interlocutore e verificare che esso sia legittimato ad ottenere quanto domandato. In particolare, nel caso di richieste da parte di terzi può essere necessario, a seconda della natura dei dati richiesti, procedere nel seguente modo:

- chiedere il nome del chiamante e la motivazione della richiesta;
- richiedere il numero di telefono da cui l'interlocutore sta effettuando la chiamata;
- verificare che il numero dichiarato corrisponda a quello del chiamante;

procedere immediatamente a richiamare la persona che ha richiesto l'informazione, con ciò accertandosi della identità dichiarata in precedenza.

Quando il dato deve essere inviato a mezzo fax, posta elettronica, SMS, ecc. e, in particolar modo, nel caso in cui vengano inviati documenti contenenti dati sensibili occorre:

- prestare la massima attenzione affinché il numero telefonico o l'indirizzo e-mail immessi siano corretti;

• verificare che non vi siano inceppamenti di carta o che dalla macchina non siano presi più fogli e attendere sempre il rapporto di trasmissione per un ulteriore verifica del numero del destinatario e della quantità di pagine inviate;

• nel caso di documenti inviati per posta elettronica accertarsi, prima di confermare l'invio, di avere allegato il file giusto;

• in caso di trasmissione di dati particolarmente delicati è opportuno anticipare l'invio chiamando il destinatario della comunicazione al fine di assicurare il ricevimento nelle mani del medesimo, evitando che terzi estranei o non autorizzati conoscano il contenuto della documentazione inviata.

Tutti coloro che provvedono alla duplicazione di documenti con stampanti, macchine fotocopiatrici o altre apparecchiature, in caso di copia erronea o non leggibile correttamente, da cui potrebbero essere desunti dati personali, sono tenuti a distruggere il documento mediante apposita macchina "distruggi documenti" o con qualunque altro mezzo che ne renda impossibile la ricostruzione in modo da escludere qualunque possibilità da parte di estranei di venire a conoscenza dei dati medesimi.

15.12 ARCHIVI CARTACEI

Tutto il materiale cartaceo contenente dati personali non deve essere lasciato incustodito sulle scrivanie e, a fine lavoro, deve essere riposto in un luogo sicuro, possibilmente in armadi chiusi a chiave. Inoltre, occorre usare la medesima perizia nello svolgimento delle normali quotidiane operazioni di lavoro, per evitare che il materiale risulti facilmente visibile a persone terze o, comunque, ai non autorizzati al trattamento.

In caso di trattamento di dati particolari (condizione di salute, dati giudiziari, ecc.), tutta la documentazione cartacea deve essere conservata in armadi/cassetti chiusi a chiave o stanze chiuse a chiave in caso di allontanamento, anche temporaneo, dalla postazione di lavoro.

L'accesso a tutti i locali aziendali deve essere consentito solo a personale preventivamente autorizzato dalla Titolarità.

Gli armai della FIABA ETS, sono muniti di serratura.

15.13 VIDEOSORVEGLIANZA

Nell'associazione FIABA ETS. non è presente un sistema di videosorveglianza e non sono presenti videocitofoni.

15.14 SISTEMI ANTINTRUSIONE

E' presente un allarme perimetrale e interno collegato con l'istituto di vigilanza e con i cellulari del titolare e del responsabile del trattamento dei dati. Sono presenti anche sensori su porte e finestre.

15.15 DISPOSITIVI ANTINCENDIO

In azienda sono presenti estintori per apparecchiature elettriche.

15.16 ALTRE MISURE ADOTTATE DALL'AZIENDA

- Aggiornamenti continui dei software
- Chiusura degli uffici a chiave
- Archiviazione cartacea in armadi chiusi a chiave
- In caso di licenziamento di un dipendente che trattava dati, si esegue un cambio password immediato e si cancella la mail del dipendente.
- I documenti archiviati non sono mai portati all'esterno dell'azienda e non sono disponibili al di fuori dell'orario di lavoro.
- Presenza di un regolamento interno per la riservatezza dei dati.
- Le cartelle mediche dei dipendenti le custodisce il medico competente.

L'azienda esternalizza solo alcuni servizi base per svolgere le sue normali attività lavorative come commercialista, consulente del lavoro, consulente paghe, RSPP, medico competente, consulenti esterni ed enti certificatori.
Si è provveduto ad inviare in via telematica la delega di collaboratori dati in outsourcing, in allegato 14.

16. TRASFERIMENTO DATI AI PAESI EXTRA UE

Il Regolamento Europeo 679/2018 prevede il divieto di trasferire dati verso titolari o responsabili in paesi extra UE, senza garanzie.
Si devono stipulare garanzie contrattuali e utilizzare deroghe al divieto di trasferimento applicabili in specifiche situazioni (es: difendere un diritto in sede giudiziaria).
Il consenso del trattamento dei dati da mandare all'interessato deve essere esplicito per poter trasferire dati a Paesi fuori dall'Unione Europea.
Bisogna verificare se ci sono i riconoscimenti di adeguatezza da parte della commissione europea e definire procedure operative sia per la verifica di adeguatezza che per le garanzie contrattuali.
FIABA ETS. ha un solo fornitore di fasi in outsourcing estero, al quale è stata inviata informativa clienti e fornitori per paesi extra UE in allegato 15.

17. ALLEGATI AL MANUALE OPERATIVO GDPR

Allegato 1 Registro trattamento dati
Allegato 2 Nomina del responsabile del trattamento dei dati personali Allegato 3
Analisi delle cause
Allegato 4 Valutazione impatto protezione dati (DPIA) Allegato 5
Informative clienti /fornitori
Allegato 6 Informativa dipendenti
Allegato 7 Informativa software house, tecnici informativi Allegato 8
Registro di richieste degli interessati
Allegato 9 Registro Data Breach
Allegato 10 Modello segnalazione Data Breach Allegato 11
Piano di formazione
Allegato 12 Organigramma GDPR
Allegato 13 Misure di sicurezza e linee guida aziendali per il trattamento dei dati personali e l'uso di internet e posta elettronica
Allegato 14 Delega collaboratori dati in outsourcing
Allegato 15 Informativa clienti e fornitori di Paesi fuori dall'Unione Europea