MANUALE PRIVACY

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)

ROMA, 21/05/2018

La **FONDAZIONE NAZIONALE SICUREZZA RUBES TRIVA** con sede Legale in Roma, Lungotevere dei Mellini n. 30 - 00193, in qualità di Titolare del Trattamento dei dati

in considerazione

dell'obbligo previsto all'art. 32 del Reg. 2016/679 di attuare misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al rischio, ritiene utile e fondamentale tenere una sorta di **Registro delle attività di trattamento** che racchiuda la politica aziendale adottata in materia.

STATUTO E ORGANI DELLA FONDAZIONE

La Fondazione Rubes Triva è un Organismo paritetico - Ente bilaterale riconosciuto che, operando nel rispetto dei principi enunciati dalla Costituzione Italiana, promuove tutte le iniziative formative e informative atte a salvaguardare l'integrità psico-fisica della persona in materia di salute e sicurezza nei luoghi di lavoro, coadiuvando le aziende di Igiene Ambientale nell'adozione di strategie volte alla diffusione della cultura della prevenzione.

La Fondazione è costituita da "UTILITALIA", "FEDERAZIONE LAVORATORI FUNZIONE PUBBLICA CGIL", "FIT CISL FEDERAZIONE ITALIANA TRASPORTI", "F.I.A.D.E.L. FEDERAZIONE ITALIANA AUTONOMA DIPENDENTI ENTI LOCALI" e "UILTRASPORTI".

Gli organi della Fondazione sono:

a. il Consiglio di Amministrazione;

b. il Presidente;

c. il Vice Presidente;

d. il Direttore;

e. il Collegio dei Revisori;

Statuto

CDA: La Fondazione è amministrata da un Consiglio di Amministrazione.
Il Consiglio di Amministrazione è composto da otto consiglieri di cui quattro, nominati su specifica designazione di UTILITALIA ed altri quattro consiglieri, su specifica designazione delle organizzazioni sindacali fondatrici.
Il Consiglio di Amministrazione resta in carica per il periodo di tempo stabilito all'atto della nomina, comunque non superiore a tre esercizi, salvo revoca o dimissioni, ed è rieleggibile; i componenti devono essere in possesso e documentare, all'atto della loro designazione, i requisiti professionali, di onorabilità e le specifiche competenze connesse con la carica da assumere.
Nei casi di decesso, dimissioni o decadenza dalla carica di uno dei componenti, il Consiglio di Amministrazione, in occasione della prima riunione, procederà all'integrazione della carica resasi vacante mediante cooptazione.
Le cooptazioni devono essere effettuate su designazione della parte o delle parti che avevano espresso la nomina dei componenti

I membri del Consiglio di Amministrazione eletti in questo modo ad integrazione dei posti vacanti dureranno in carica fino alla scadenza del mandato dei membri originariamente eletti. Ove la decadenza o le dimissioni riguardassero almeno la metà dei componenti del Consiglio di Amministrazione, il Consiglio stesso decadrà e il Presidente o il Vice Presidente provvederà alla convocazione delle parti fondatrici.

Il Consiglio di Amministrazione nomina il Presidente e il Vice Presidente scegliendoli alternativamente tra i consiglieri designati da UTILITALIA e dalle organizzazioni sindacali fondatrici.

Il Consiglio di Amministrazione può nominare un Presidente Onorario tenuto conto della particolare rappresentatività della persona.

Il Consiglio di Amministrazione provvede all'amministrazione ordinaria e straordinaria delle attività della Fondazione.

Al Consiglio di Amministrazione in particolare spetta:

a) approvare entro il mese di dicembre il conto preventivo dell'anno seguente ed entro il mese di maggio il bilancio dell'anno precedente;

b) stabilire le linee programmatiche della Fondazione;

c) deliberare eventuali modifiche statutarie;

d) deliberare sullo scioglimento della Fondazione e sulla devoluzione del patrimonio;

e) emanare regolamenti interni che non siano in contrasto con il presente statuto;

f) deliberare gli eventuali provvedimenti attinenti agli scopi e finalità statutarie, dettati da carattere di urgenza e necessità;

g) nominare il Collegio dei Revisori, di cui all'art. 12, su indicazione dei soci fondatori, individuandone il Presidente;

h) nominare il Direttore della Fondazione, su specifica designazione di UTILITALIA, al fine di coordinare e gestire le attività proprie della Fondazione stessa, determinandone il ruolo, la mansione, le deleghe ed i compensi.

Le delibere del Consiglio di Amministrazione sono valide se è presente la maggioranza dei membri in carica e sono prese a maggioranza dei ¾ dei presenti.

Il Consiglio di Amministrazione è convocato dal Presidente, o, in caso di suo impedimento, dal Vicepresidente, ogni volta lo ritenga necessario, con avviso da spedire almeno 5 (cinque) giorni prima di quello stabilito per l'adunanza, anche a mezzo fax o e-mail.

In caso di urgenza è consentita la convocazione anche telefonica, via e-mail o telegrafica, purché effettuata con preavviso di almeno 2 (due) giorni.

Il Consiglio di Amministrazione può essere convocato, con le medesime modalità sopra indicate, anche su espressa richiesta di almeno 3 dei componenti del Consiglio medesimo, i quali dovranno indicare anche gli argomenti da discutere.

In ogni caso il Consiglio di Amministrazione dovrà riunirsi almeno due volte l'anno.

I verbali delle deliberazioni del Consiglio di Amministrazione devono essere trascritti in ordine cronologico su apposito registro e devono essere sottoscritti dal Presidente e dal segretario dell'adunanza del Consiglio.

I membri del Consiglio di Amministrazione che senza giustificato motivo non intervengono per 3 (tre) sedute consecutive possono essere dichiarati decaduti con deliberazione del Consiglio stesso.

Il Consiglio di Amministrazione nomina, su proposta del Presidente, i membri della Commissione Valutativa per l'Asseverazione dei Modelli Organizzativi e di Gestione della SSL, del Comitato etico e dell'Osservatorio della Ricerca, la divulgazione e la formazione e provvede a determinarne i compiti.

Presidente e Vice Presidente: Il Presidente ha la rappresentanza legale della Fondazione di fronte a terzi ed in giudizio.

Inoltre il Presidente:

a) convoca il Consiglio di Amministrazione e lo presiede proponendo le materie da trattare nelle relative adunanze;

b) sorveglia il buon andamento amministrativo della Fondazione;

c) cura l'osservanza dello statuto e ne promuove la riforma qualora si renda necessario;

d) adotta in caso di urgenza ogni provvedimento opportuno riferendo nel più breve tempo al Consiglio.

Il Vice Presidente presiede il Consiglio di Amministrazione in caso di assenza e impedimento del Presidente e per i medesimi motivi subentra nelle funzioni e poteri attribuiti al Presidente.

Il Direttore: Il Direttore è nominato dal Consiglio di Amministrazione, su specifica designazione dei rappresentanti di UTILITALIA, che ne stabilisce la natura, la qualifica, la durata dell'incarico e il relativo compenso.

Il Direttore è il responsabile operativo della Fondazione.

Egli in particolare:

a) provvede alla gestione organizzativa ed amministrativa della Fondazione, nonché alla organizzazione e promozione delle singole iniziative, predisponendo mezzi e strumenti necessari per la loro concreta attuazione;

b) dà esecuzione, nelle materie di sua competenza, alle deliberazioni del Consiglio di Amministrazione, nonché agli atti del Presidente;

c) su parere della Commissione Valutativa per l'Asseverazione dei Modelli Organizzativi e di Gestione della SSL, delibera il documento di asseverazione degli stessi.

Il Direttore partecipa, senza diritto di voto, alle riunioni del Consiglio di Amministrazione.

Collegio dei Revisori: Il Collegio dei Revisori è composto da 3 (tre) membri effettivi e da 2 (due) supplenti ai sensi dell'art. 2397 del Codice Civile. Il Collegio dei Revisori è eletto dal Consiglio di Amministrazione e resta in carica tre esercizi scadendo, di conseguenza, alla data della riunione convocata per l'approvazione del bilancio consuntivo relativo al terzo esercizio dell'incarico.

Il Consiglio di Amministrazione, all'atto della nomina, determinerà anche il compenso spettante ai Revisori effettivi per l'intera durata del loro ufficio e/o a quant'altro richiesto dalla legge.

I membri effettivi del Collegio dei Revisori sono nominati:

a) uno con funzione di Presidente, di comune accordo tra i componenti il Collegio, alternativamente su designazione di UTILITALIA e delle organizzazioni sindacali fondatrici;

b) uno effettivo, designato dalle organizzazioni sindacali fondatrici;

c) uno effettivo, designato dai rappresentanti di UTILITALIA.

Le predette organizzazioni sindacali e UTILITALIA designano altresì due Revisori supplenti, uno per parte, destinati a sostituire i revisori eventualmente dimissionari.

Il Collegio può partecipare a tutte le riunioni del Consiglio di Amministrazione ed esprimere il proprio parere sugli argomenti in discussione, ma senza diritto di voto.

Il Collegio dei Revisori deve controllare l'amministrazione della Fondazione, vigilare sull'osservanza delle norme di legge e dello statuto, accertare la regolare tenuta della contabilità, nonché la corrispondenza di questa ai bilanci consuntivi su cui presenterà annualmente al Consiglio di Amministrazione la propria relazione.

PREMESSA

La Fondazione, per lo svolgimento dell'attività professionale, detiene archivi elettronici e cartacei contenenti dati personali ed è nostra intenzione pertanto raccogliere e custodire tali dati 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 consentito o non conforme alle finalità di raccolta.
Proprio ai fini della nostra attività professionale, la Fondazione viene in contatto e tratta dati personali:

- dei propri clienti;
- dei propri collaboratori;
- dei propri dipendenti.

ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

In questa sezione verranno descritti i principali eventi potenzialmente dannosi per la sicurezza dei dati e valutate le possibili conseguenze e la gravità in relazione al contesto fisico-ambientale di riferimento e agli strumenti elettronici utilizzati.

Verranno presi in considerazione i seguenti eventi:

1. COMPORTAMENTO DEGLI OPERATORI:

   - Sottrazione di credenziali di autenticazione
   - Carenza di consapevolezza, disattenzione o incuria
   - Comportamenti sleali o fraudolenti
   - Errore materiale

2. EVENTI RELATIVI AGLI STRUMENTI:

   - Azione di virus informatici o di programmi suscettibili di recare danno
   - Spamming o tecniche di sabotaggio
   - Malfunzionamento, indisponibilità e degrado degli strumenti
   - Accessi esterni non autorizzati
   - Intercettazione di informazioni in rete

3. EVENTI RELATIVI AL CONTESTO FISICO-AMBIENTALE:

   - Ingressi non autorizzati a locali/aree ad accesso ristretto
   - Sottrazioni di strumenti contenente dati
   - Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali,...), nonché dolosi, accidentali o dovuti ad incuria
   - Guasto a sistemi complementari (impianto elettrico, climatizzazione, ecc.)
   - Errori umani nella gestione della sicurezza fisica

Una volta individuati gli eventi potenzialmente dannosi per la sicurezza dei dati verrà valutata l'IMPATTO SULLA SICUREZZA, cioè verranno descritte le principali conseguenze individuate per la sicurezza dei dati, in relazione a ciascun evento, e valutata la loro gravità anche in relazione alla rilevanza e alla probabilità stimata dell'vento (in termini: alta/media/bassa).

In questo modo è possibile formulare un primo indicatore omogeneo per i diversi rischi da contrastare.

L'analisi dei rischi è esplicitata nelle tabelle seguenti.

Tabella 1 (analisi dei rischi in base all'evento: *comportamento degli operatori*)

RISCHI		SI		NO	Descrizione dell'impatto sulla sicurezza (gravità: alta/media/bassa)
		Probabile	Improbabile		
Comportamenti degli operatori	Sottrazione di credenziali di autenticazione		X		ALTO
	Carenza di consapevolezza, disattenzione o incuria		X		MEDIO
	Comportamenti sleali o fraudolenti		X		ALTO
	Errore materiale		X		MEDIO
	Altro evento				

Tabella 2 (analisi dei rischi in base agli: *eventi relativi agli strumenti*)

RISCHI		SI		NO	Descrizione dell'impatto sulla sicurezza (gravità: alta/media/bassa)
		Probabile	Improbabile		
Eventi relativi agli strumenti	Azione di virus informatici o di programmi suscettibili di recare danno	X			ALTO
	Spamming o tecniche di sabotaggio		X		MEDIO
	Malfunzionamento, indisponibilità e degrado degli strumenti	X			BASSO
	Accessi esterni non autorizzati		X		BASSO
	Intercettazione di informazioni in rete	X			ALTO
	Altro evento				

Tabella 3 (analisi dei rischi in base agli: *eventi relativi al contesto fisico-ambientale*)

RISCHI		SI		NO	Descrizione dell'impatto sulla sicurezza (gravità: alta/media/bassa)
		Probabile	Improbabile		
Eventi relativi al contesto fisico-ambientale	Ingressi non autorizzati a locali/aree ad accesso ristretto		X		BASSO
	Sottrazioni di strumenti contenente dati		X		BASSO
	Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali,...), nonché dolosi, accidentali o dovuti ad incuria		X		BASSO
	Guasto a sistemi complementari (impianto elettrico, condizionatore ecc.)	X			BASSO
	Errori umani nella gestione della sicurezza fisica		X		BASSO
	Altro evento				

DEFINIZIONI GENERALI DEL REG. 2016/679

Ai fini del presente regolamento s'intende per:

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

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

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

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

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

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

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

8) «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

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

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

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

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

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

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

15) «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

16) «stabilimento principale»:

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

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

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

18) «impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le Fondazione 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;

ORGANIGRAMMA

PRESIDENTE
Massimo Cenciotti

VICE PRESIDENTE
Daniele Fortini

DIRETTORE
Giuseppe Mulazzi

CONSIGLIO DI AMMINISTRAZIONE
Filippo Brandolini
Annamaria Caputi
Angelo Curcio
Gianfranco Grandaliano
Claudio Tarlazzi
Luigi Verzicco

COLLEGIO DEI REVISORI DEI CONTI
Presidente
Giovanni Pizzolla

Revisori
Vico Valentino Gabriele
Massimo Melone

TITOLARE DEL TRATTAMENTO: Giuseppe Mulazzi in qualità di Direttore.

I membri del CDA hanno unanimemente approvato la documentazione nei consigli tenutisi il 07/06/2017 e 22/03/2018.

AMMINISTRATORE DI SISTEMA: Massimiliano Spadi in qualità di dipendente.

La Fondazione ha nominato incaricati del trattamento dati i dipendenti nelle persone di:

- BIGLIARDI MONICA, nella sua qualità di dipendente;
- RIZZO STEFANIA, nella sua qualità di dipendente;
- SPADI MASSIMILIANO, nella sua qualità di dipendente;
- CASAI LUCA, nella sua qualità di consulente;
- RAMAZZINI NADIA, nella sua qualità di consulente;

La Struttura Organica della Fondazione

Direzione Generale
Giuseppe Mulazzi

Tel: 06 32 690 411 Fax: 06 32 22 595
mail: segreteria@fondazionerubestriva.it

Coordinazione Progetti
Direzione e Amministrazione
Monica Bigliardi
Tel: 06 92 08 35 24 Fax: 06 32 22 595
mail: segreteria@fondazionerubestriva.it
PEC: fondazionerubestriva@pec.it

Segreteria e Amministrazione
Stefania Rizzo

Tel: 06 32 690 411 Fax: 06 32 22 595
mail: fondazione@fondazionerubestriva.it

Webmaster
Massimiliano Spadi

Tel: 06 92 08 36 31 Fax: 06 32 22 595
mail: info@fondazionerubestriva.it

Ricerca e Gestione Piani Formativi
Nadia Ramazzini

Tel: 06 92 08 36 61 Fax: 06 32 22 595
mail: ramazzini@fondazionerubestriva.it

Formazione
Luca Casai

Tel: 06 92 08 36 87 Fax: 06 32 22 595
mail: casai@fondazionerubestriva.it

Le banche dati sono suddivise sulla base dei compiti affidati ad ogni dipendente. Chi ha accesso ad una banca dati, non ha accesso alle altre che non gli competono.

In allegato elenco banche dati e accessi.

Unico software in dotazione è quello di contabilità che viene affidata alla studio Ragionier Tiziano Galusi, nominato Responsabile esterno del trattamento.

LA SICUREZZA DEI DATI (PRIVACY BY DESIGN e PRIVACY BY DEFAULT)

Alla luce dei rischi individuati, la Fondazione si è posta come obiettivo quello di mettere in atto le misure tecniche ed organizzative necessarie per garantire un livello di sicurezza adeguato al rischio.

In particolare, la Fondazione innanzitutto tratta i dati rispettando i principi esplicitamente indicati nell'art. 5 del Reg. 2016/679 ossia:

- **Liceità, correttezza, trasparenza: ogni trattamento è esplicitamente indicato nell'informativa;**
- **Limitazione delle finalità: le finalità sono quelle di utilità sociale con attività prevalente nel settore della formazione;**
- **Minimizzazione dei dati e, dove possibile, pseudonimizzazione: i dati trattati sono soltanto quelli necessari per l'erogazione del piano formativo;**
- **Esattezza dei dati: i dati sono inseriti direttamente dall'azienda;**
- **Limitazione della conservazione: il tempo di conservazione dei dati è in genere quello della durata della sottoscrizione al CCNL. La Fondazione tuttavia tratta alcuni dati anche a fini di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 e per questi prevede un esplicito consenso.**
- **Integrità e riservatezza attraverso le misure adottate per la protezione dei dati stessi.**

La prima e fondamentale misura per garantire la sicurezza dei dati è l'informativa privacy: l'informativa ex art. 13 del Regolamento 2016/679 continua a rappresentare il fulcro per poter trattare i dati di una persona fisica.

- La Fondazione prevede una informativa per i clienti, riportata nell'**Allegato A**, che spedisce all'azienda anteriormente al trattamento del dato stesso. La Fondazione entra in contatto con i dati aziendali – soprattutto dei dipendenti – solo al momento della compilazione del gestionale da parte dell'azienda stessa.

Dunque l'iter procedurale è il seguente: l'azienda aderisce al CCNL o richiede volontariamente di accedere al software di gestione della formazione. In entrambi i casi, la Fondazione provvederà all'invio dell'informativa privacy e all'incarico del dipendente aziendale che materialmente avrà accesso al software. Sarà poi onere dell'azienda stessa nominare la Fondazione Responsabile esterno del trattamento per l'accesso in remoto all'interno del gestionale.

In ogni caso, anche nelle istruzioni del software, viene esplicitamente detto che la Fondazione entra in remoto e vede i dati aziendali e quindi è presente un'autorizzazione dell'azienda a tale trattamento.

- La Fondazione prevede una informativa per i dipendenti, riportata nell'**Allegato B**, da inserire nel contratto di assunzione.

Quando il consenso al trattamento dei dati è necessario, la Fondazione prevede una esplicita richiesta che viene successivamente archiviata.

Procedura Data Breach:

In caso di incidente fisico-tecnico, tra le misure adottate, è presente quella di ripristinare tempestivamente la disponibilità e l'accesso dei dati stessi.
Alla luce dell'art. 33, il *data breach* - ossia la violazione di sicurezza che comporta la distruzione, perdita, divulgazione non autorizzata dei dati stessi - fa scattare un obbligo di notifica al Garante Privacy, al massimo entro 72 ore dalla scoperta di essa.

Quando la violazione è suscettibile di presentare un rischio elevato per le persone fisiche inoltre, il Titolare comunica la violazione anche all'interessato.

In allegato modulo segnalazione.

DIRITTI DELL'INTERESSATO

Alla luce degli articoli 15 e ss. Del Regolamento, vari sono i diritti dell'interessato e la nostra Fondazione prevede una procedura per dare loro una piena e tempestiva risposta.

- **Diritto di accesso ai propri dati personali (art. 15);**
- **Diritto di rettifica (art. 16);**
- **Diritto alla cancellazione dei dati (cd. Diritto all'oblio), senza ritardo ingiustificato qualora ricorrano determinate motivazioni previste per legge (art 17);**
- **Diritto di limitazione di trattamento (art. 18);**
- **Diritto alla portabilità dei dati ossia il diritto di trasmettere dati da un Titolare ad un altro Titolare senza impedimenti (art. 20);**
- **Diritto di opposizione al trattamento (art. 21) anche ai fini di profilazione;**
- **Diritto ad ottenere un processo decisionale non completamente automatizzato (art. 22).**

È previsto che, in caso di reclamo da parte di un interessato sulla base dei diritti appena elencati, il Direttore – Titolare del Trattamento - provveda immediatamente a dare seguito alla richiesta.
Sulla base dell'informativa ex art. 13, il Direttore viene infatti informato della richiesta attraverso mail e metterà in moto il meccanismo necessario alla misura prevista.
Se i dati vengono poi trasferiti ad altri, il Direttore comunica a questi le eventuali rettifiche o cancellazioni o limitazioni di trattamento.

PROTEZIONE DELLE AREE E DEI LOCALI

DATI CARTACEI

L'area contenente dati in supporto cartaceo è ubicata in modo tale che ciascun addetto possa rilevare a vista il tentativo di accesso da parte di persone estranee e, di conseguenza, impedirne l'accesso stesso.

L'ubicazione di stampante ed apparecchio fax tradizionale non consente ad estranei di leggere od asportare eventualmente documenti; l'area contenente stampante ed apparecchio fax è ubicata in modo tale che ciascun addetto possa rilevare a vista il tentativo di accesso da parte di persone estranee e, di conseguenza, impedirne l'accesso stesso.

La Fondazione ha diversi armadi chiusi a chiave per l'archiviazione di dati personali.

DATI ELETTRONICI

I dati di tipo informatico vengono gestiti da 3 PC e protetti tramite l'utilizzo di passwords: le passwords sono costituite da 8 caratteri alfanumerici e vengono cambiate automaticamente ogni sei mesi. Solo i computer che trattano dati sensibili aggiornano, automaticamente, la password ogni 3 mesi.

Ogni dipendente ha unicamente la password del PC che utilizza in modo che ognuno, a seconda delle mansioni svolte all'interno della Fondazione, possa accedere solo a determinati tipi di documenti, come da allegato "Permessi utenti per cartelle del server".

Tutta l'amministrazione lavora direttamente nel server.
La Fondazione ha una rete di ufficio e una VPN per il collegamento in remoto.
Il salvataggio avviene sia sul server sia su altri due supporti: uno in un hard disk del pc e un'altra copia dell'ADS in altro hard disk.

È stato acquistato anche un Cloud– Google suite.

L'amministratore di sistema, già nominato, verifica che il backup sia andato a buon fine.
L'amministratore di sistema, quando accede per la manutenzione o il riavvio di qualche malfunzionamento, non ha accesso ai dati che sono protetti attraverso password.

CRITERI E PROCEDURE ADOTTATI PER ASSICURARE L'INTEGRITÀ DEI DATI

- Il sito internet rispetta le norme di legge in particolare in tema di cookies e informativa.

Computer e supporti informatici:

1. I computer risultano sollevati da terra, in modo da evitare eventuali perdite di dati dovuti ad allagamenti, ecc.;

2. L'integrità dei dati è inoltre garantita mediante idonee procedure di salvataggio periodico (backup).

3. L'introduzione di password all'accensione del personal computer determina un livello di sicurezza, circa i dati contenuti nei PC, ritenuto più che soddisfacente. L'introduzione di dette password ha inibito ad estranei l'uso dei personal computer, attraverso i quali, si accede alla posta elettronica;

4. In merito a messaggi e-mail inviati a più destinatari, quale mittente dovrà essere indicata la nostra Fondazione con il nostro indirizzo e-mail, ed in Ccn i destinatari (che in tal modo non possono individuare gli indirizzi e-mail degli altri destinatari, attraverso la funzione di proprietà) salvo richieste esplicite di clienti e/o fornitori;

5. Nei messaggi di posta inviati viene digitata la seguente dicitura: "*in ottemperanza al Reg. UE 2016/679 le informazioni contenute in questo messaggio di posta elettronica sono destinate esclusivamente agli individui e agli enti ai quali risulta indirizzato. Il suo contenuto (inclusi gli allegati) sono confidenziali e riservati: se Lei non è tra i destinatari originari non deve utilizzare, rivelare, trasmettere, copiare né stampare il suo contenuto; se Lei ha ricevuto questo messaggio di posta elettronica per errore, è pregato di avvisarci inviando un messaggio di posta elettronica all'indirizzo del mittente, e quindi cancellare e distruggere il messaggio dal Suo sistema*";

6. I supporti magnetici contenenti dati, possono essere riutilizzati esclusivamente previa formattazione irreversibile, in modo da impedire la letture dei dati precedenti;

7. Tutti i giorni, in orario di chiusura, i pc vanno in modalità stand-by. Dunque per la riattivazione è necessaria la password.

8. I Personal Computer sono dotati di antivirus, che vengono aggiornati automaticamente. Anche il server di rete è dotato di un antivirus, questo per avere un doppio controllo e una maggiore sicurezza;

9. È presente un firewall.

Supporti cartacei:

Relativamente ai supporti cartacei, i criteri di protezione dei dati debbono essere ricercati nei seguenti:

1. Qualsiasi documento in entrata/uscita dalla Fondazione appartenenti a clienti/fornitori/consulenti/dipendenti/ecc. viene inserito in apposite cartelline non trasparenti, raccoglitori o buste;

2. Le eventuali rubriche telefoniche in utilizzo su supporto cartaceo sono richiuse dopo la consultazione in armadi o cassettiere, che dopo l'orario di lavoro saranno chiuse a chiave;

3. Le copie dei fax inviati e ricevuti dovranno essere archiviati in appositi raccoglitori che successivamente verranno archiviati in armadi;

4. Nella pagine accompagnatoria dei Fax viene digitata la seguente dicitura: "*in ottemperanza al Reg. UE 2016/679 le informazioni contenute in questo fax sono destinate esclusivamente agli individui e agli enti ai quali risulta indirizzato. Il suo contenuto (inclusi gli allegati) sono confidenziali e riservati: se Lei non è tra i destinatari originari non deve utilizzare, rivelare, trasmettere, copiare né stampare il suo contenuto; se Lei ha ricevuto questo fax per errore, è pregato di avvisarci e quindi distruggere il documento*";

5. Tutti gli archivi cartacei sono chiusi all'interno di raccoglitori inseriti negli armadi chiusi a chiave;

6. Tutti gli archivi cartacei relativi ai dipendenti sono chiusi all'interno di raccoglitori inseriti in un apposito armadio chiuso a chiave;

7. Tutti i curricula vitae ricevuti in forma cartacea vengono archiviati in un'apposita cartellina e chiusi in un armadio in ufficio che, al termine dell'orario di lavoro, viene chiuso a chiave; l'utilizzazione di tale documentazione è consentita esclusivamente a personale autorizzato.

CRITICITA' EMERSE: MISURE IN VIA DI ADOZIONE

Il sottoscritto è impegnato inoltre a perfezionare le misure già adottate tramite:

- Analisi e valutazione continua e sistematica delle misure adottate;
- Valutazione dell'applicazione del nuovo Regolamento europeo e adeguamento ai provvedimenti del Garante Privacy;
- Responsabilizzazione massima di tutti gli operatori anche tramite interventi formativi ed informativi;
- Distruggi documenti

CONCLUSIONI

Il presente documento scaturisce da un'analisi di valutazione dei rischi aziendali ed è prevista una procedura per testare, verificare e valutare regolarmente l'efficacia del sistema in questione per garantire sempre un più alto livello di sicurezza ed efficace attuazione delle misure tecniche ed organizzative.
Il Manuale è a disposizione in Fondazione per qualsiasi dipendente o collaboratore voglia consultarlo e ognuno è tenuto, in base ai propri incarichi, al suo pieno rispetto.
Ogni anno, nel periodo di marzo, si tiene una riunione di istruzione degli incaricati al trattamento per renderli edotti delle misure adottate per la sicurezza del trattamento dati e per la prevenzione dei rischi di anomalie al trattamento stesso.
La formazione annuale è avvenuta in data 2 maggio 2018.

IL TITOLARE DEL TRATTAMENTO

GIUSEPPE MULAZZI

Consiglio di Amministrazione tenutosi in data 07/06/2017 e 22/03/2018.