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)

e

D.LGS. 196/2003 vigente dopo le modifiche del D.LGS. 101/2018 recante Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016.

ROMA, 30.09.2019

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 - C.F. 97598620587
segreteria@fondazionerubestriva.it fondazionerubestriva@pec.it
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 e in considerazione della necessaria "responsabilizzazione" (accountability) sottolineata dal Regolamento ritiene fondamentale tenere una sorta di Registro delle attività di trattamento che racchiuda la politica aziendale adottata in materia tale da dimostrare l'adozione di comportamenti proattivi e di misure finalizzate ad assicurare l'applicazione del regolamento stesso.

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 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 (19);

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.

DESCRIZIONE ATTIVITÀ LAVORATIVA

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 dimissionari o decaduti.

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 stato nominato con verbale del 10.05.2010 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.

FONDAZIONE
RUBES TRIVA
SICUREZZA. LAVORO. AMBIENTE

ATTIVITA'

La Fondazione si occupa di promuovere le iniziative formative 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.

In particolare la Fondazione mette a disposizione delle aziende che aderiscono al CCNL o a quelle che, pur non aderendo al CCNL, lo richiedono, un software di gestione della formazione.

Attraverso username e password, la Fondazione concede la possibilità alle Aziende di gestire tutta l'attività formativa attraverso tale gestionale.

Dunque la Fondazione è titolare del trattamento dei dati aziendali necessari per la concessione delle credenziali ma è responsabile del trattamento per quanto riguarda i dati dei dipendenti dell'azienda stessa, primo fra tutti colui che materialmente sarà incaricato dall'azienda di accedere al software per implementarlo.

Oltre all'attività formativa, la Fondazione si occupa della consulenza aziendale in materia di sicurezza sul lavoro attraverso il proprio personale o attraverso consulenti esterni.

FONDAZIONE
RUBES TRIVA
SICUREZZA. LAVORO. AMBIENTE

REGISTRO DEI TRATTAMENTI TITOLARE DEL TRATTAMENTO

SCHEDA REGISTRO DEI TRATTAMENTI
Ultimo aggiornamento 30.09.2019

TITOLARE *FONDAZIONE NAZIONALE SICUREZZA RUBES TRIVA*

RESPONSABILE DELLA PROTEZIONE DEI DATI *MONICA BIGLIARDI*

TIPOLOGIA DI TRATTAMENTO	FINALITA' E BASE GIURIDICA	CATEGORIE DI INTERESSATI	CATEGORIE DI DATI PERSONALI	CATEGORIE DI DESTINATARI *[indicare eventuali responsabili del trattamento o altri titolari cui i dati siano comunicati]*	TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI *[indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le "garanzie" adottate ai sensi del capo V del RGPD]*	TERMINI ULTIMI DI CANCELLAZIONE PREVISTI	MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE
Raccolta Registrazione Organizzazione Strutturazione Conservazione Adattamento Modifica Consultazione Elaborazione Selezione Estrazione Raffronto Utilizzo Comunicazione Limitazione Cancellazione **MODALITA':** cartacea ed elettronica	**Gestione del personale** Gestione del patrimonio mobiliare ed immobiliare adempimento obblighi fiscali e contabili Utilità sociale **Gestione della clientela** gestione dei fornitori gestione del contenzioso programmazione delle attività Servizi a tutela di consumatori e utenti **Marketing** Corsi e eventi rilevazione grado di soddisfazione del cliente attraverso test finali anonimi **attività di consulenza** archiviazione nel pubblico interesse, ricerca storica o scientifico fini statistici **BASE GIURIDICA** 1. Consenso 2. Contratto 3. Obbligo legale del Titolare	Clienti: aziende; Soci; Revisori; Dipendenti; Lavoratori autonomi Candidati per futuro rapporto lavorativo Fornitori.	**Dati comuni:** - codice fiscale/partita iva e altri numeri identificativi - attività economiche, commerciali, finanziarie e assicurative - mail - sesso - ruolo ricoperto in azienda	Membri del CDA e Revisori contabili; Studi Professionali per la consulenza; Docenti formatori; Enti di ricerca – ad es. Università; Inail/ISS.	NO	Clienti: periodo di sottoscrizione del CCNL o fino a richiesta di cancellazione. Dipendenti: periodo di durata del contratto e tenuta successiva ai soli fini dimostrativi e di contenzioso	**MISURE FISICHE** - Armadi chiusi a chiave - Cassaforte - Allarme - Distruggi documenti - Cartelline non leggibili - Contenitori sigillati - Controllo accessi - Estintori **MISURE LOGICHE** - Anonimizzazione **STRUMENTI ELETTRONICI** - Password - Back-up - Antivirus - Firewall - Windows aggiornato

FONDAZIONE
RUBES TRIVA
SICUREZZA. LAVORO. AMBIENTE

REGISTRO DEI TRATTAMENTI DELL'UFFICIO AMMINISTRAZIONE

SCHEDA REGISTRO DEI TRATTAMENTI
Ultimo aggiornamento 30.09.2019

TITOLARE *FONDAZIONE NAZIONALE SICUREZZA RUBES TRIVA*

RESPONSABILE DELLA PROTEZIONE DEI DATI *MONICA BIGLIARDI*

TIPOLOGIA DI TRATTAMENTO	FINALITA' E BASE GIURIDICA	CATEGORIE DI INTERESSATI	CATEGORIE DI DATI PERSONALI	CATEGORIE DI DESTINATARI *[indicare eventuali responsabili del trattamento o altri titolari cui i dati siano comunicati]*	TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI *[indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le "garanzie" adottate ai sensi del capo V del RGPD]*	TERMINI ULTIMI DI CANCELLAZIONE PREVISTI	MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE
Raccolta Registrazione Organizzazione Strutturazione Conservazione Adattamento Modifica Consultazione Elaborazione Selezione Estrazione Raffronto Utilizzo Comunicazione Limitazione Cancellazione **MODALITA':** cartacea ed elettronica	**Gestione del personale** Gestione del patrimonio mobiliare ed immobiliare adempimento obblighi fiscali e contabili **Gestione della clientela** gestione dei fornitori gestione del contenzioso programmazione delle attività Servizi a tutela di consumatori e utenti Utilità sociale **Marketing** Corsi e eventi rilevazione grado di soddisfazione del cliente attraverso test finali anonimi **attività di consulenza** archiviazione nel pubblico interesse, ricerca storica o scientifico fini statistici **BASE GIURIDICA** 1. Consenso 2. Contratto 3. Obbligo legale del Titolare	Clienti: aziende; Soci; Revisori; Dipendenti; Lavoratori autonomi Candidati per futuro rapporto lavorativo Fornitori.	**Dati comuni:** - codice fiscale/partita iva e altri numeri identificativi - attività economiche, commerciali, finanziarie e assicurative - mail - sesso - ruolo ricoperto in azienda	Membri del CDA e Revisori contabili; Studi Professionali per la consulenza; Docenti formatori; Enti di ricerca – ad es. Università; Inail/ISS.	NO	Clienti: periodo di sottoscrizione del CCNL o fino a richiesta di cancellazione. Dipendenti: periodo di durata del contratto e tenuta successiva ai soli fini dimostrativi e di contenzioso	**MISURE FISICHE** - Armadi chiusi a chiave - Cassaforte - Allarme - Distruggi documenti - Cartelline non leggibili - Contenitori sigillati - Controllo accessi - Estintori **MISURE LOGICHE** - Anonimizzazione **STRUMENTI ELETTRONICI** - Password - Back-up - Antivirus - Firewall - Windows aggiornato

FONDAZIONE
RUBES TRIVA
SICUREZZA. LAVORO. AMBIENTE

REGISTRO DEI TRATTAMENTI WEBMASTER

SCHEDA REGISTRO DEI TRATTAMENTI
Ultimo aggiornamento 30.09.2019

TITOLARE *FONDAZIONE NAZIONALE SICUREZZA RUBES TRIVA*

RESPONSABILE DELLA PROTEZIONE DEI DATI *MONICA BIGLIARDI*

TIPOLOGIA DI TRATTAMENTO	FINALITA' E BASE GIURIDICA	CATEGORIE DI INTERESSATI	CATEGORIE DI DATI PERSONALI	CATEGORIE DI DESTINATARI *[indicare eventuali responsabili del trattamento o altri titolari cui i dati siano comunicati]*	TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI *[indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le "garanzie" adottate ai sensi del capo V del RGPD]*	TERMINI ULTIMI DI CANCELLAZIONE PREVISTI	MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE
Conservazione Consultazione Utilizzo **MODALITA':** cartacea ed elettronica	**Gestione della clientela** Gestione del sito Gestione del software **BASE GIURIDICA** 1. Consenso 2. Contratto 3. Obbligo legale del Titolare	Clienti: Aziende.	**Dati comuni:** - codice fiscale/partita iva e altri numeri identificativi - attività economiche, commerciali, finanziarie e assicurative - mail - sesso - ruolo ricoperto in azienda		NO	Clienti: periodo di sottoscrizione del CCNL o fino a richiesta di cancellazione.	**MISURE FISICHE** - Armadi chiusi a chiave - Cassaforte - Allarme - Distruggi documenti - Cartelline non leggibili - Contenitori sigillati - Controllo accessi - Estintori **MISURE LOGICHE** - Anonimizzazione **STRUMENTI ELETTRONICI** - Password - Back-up - Antivirus - Firewall - Windows aggiornato

FONDAZIONE
RUBES TRIVA
SICUREZZA. LAVORO. AMBIENTE

REGISTRO DEI TRATTAMENTI CONSULENTI

SCHEDA REGISTRO DEI TRATTAMENTI
Ultimo aggiornamento 30.09.2019

TITOLARE *FONDAZIONE NAZIONALE SICUREZZA RUBES TRIVA*

RESPONSABILE DELLA PROTEZIONE DEI DATI *MONICA BIGLIARDI*

TIPOLOGIA DI TRATTAMENTO	FINALITA' E BASE GIURIDICA	CATEGORIE DI INTERESSATI	CATEGORIE DI DATI PERSONALI	CATEGORIE DI DESTINATARI *[indicare eventuali responsabili del trattamento o altri titolari cui i dati siano comunicati]*	TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI *[indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le "garanzie" adottate ai sensi del capo V del RGPD]*	TERMINI ULTIMI DI CANCELLAZIONE PREVISTI	MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE
Raccolta Registrazione Organizzazione Strutturazione Conservazione Adattamento Modifica Consultazione Elaborazione Selezione Estrazione Raffronto Utilizzo Comunicazione Diffusione Limitazione Cancellazione **MODALITA':** cartacea ed elettronica	**Gestione della clientela e dei fornitori (es. docenti)** **Attività di consulenza** **BASE GIURIDICA** Utilità sociale **NB: solo in caso di dati sensibili:** Il trattamento di categorie particolari di dati personali è vietato a meno che non ricorra una delle seguenti casistiche: trattamento effettuato da fondazione, associazione o altro organismo senza scopo di lucro	Clienti: aziende; Fornitori	**Dati comuni:** - codice fiscale/partita iva e altri numeri identificativi - attività economiche, commerciali, finanziarie e assicurative - mail - sesso - ruolo ricoperto in azienda	Membri del CDA e Revisori contabili; Studi Professionali per la consulenza; Docenti formatori; Enti di ricerca – ad es. Università; Inail/ISS.	NO	Clienti: periodo di sottoscrizione del CCNL Dipendenti: periodo di durata del contratto e tenuta successiva ai soli fini dimostrativi e di contenzioso	**MISURE FISICHE** - Armadi chiusi a chiave - Armadi ignifughi - Cassaforte - Allarme - Vigilanza - Distruggi documenti - Cartelline non leggibili - Contenitori sigillati - Controllo accessi - Badge - Videosorveglianza - Estintori **MISURE LOGICHE** - Cifratura - Pseudonimizzazione **STRUMENTI ELETTRONICI** - Password - Back-up - Antivirus - firewall - Windows

FONDAZIONE
RUBES TRIVA
SICUREZZA. LAVORO. AMBIENTE

REGISTRO TRATTAMENTI SITO INTERNET

SCHEDA REGISTRO DEI TRATTAMENTI
Ultimo aggiornamento 30.09.2019

TITOLARE *FONDAZIONE NAZIONALE SICUREZZA RUBES TRIVA*

RESPONSABILE DELLA PROTEZIONE DEI DATI *MONICA BIGLIARDI*

TIPOLOGIA DI TRATTAMENTO	FINALITA' E BASE GIURIDICA	CATEGORIE DI INTERESSATI	CATEGORIE DI DATI PERSONALI	CATEGORIE DI DESTINATARI *[indicare eventuali responsabili del trattamento o altri titolari cui i dati siano comunicati]*	TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI *[indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le "garanzie" adottate ai sensi del capo V del RGPD]*	TERMINI ULTIMI DI CANCELLAZIONE PREVISTI	MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE
Registrazione Organizzazione Conservazione Modifica Elaborazione Selezione Estrazione Raffronto Utilizzo Comunicazione Limitazione Cancellazione **MODALITA':** elettronica	**Gestione della clientela** Comunicazione delle attività in programma; Comunicazione di articoli e riviste informative; Servizi a tutela di consumatori e utenti. **Marketing** Corsi e eventi **BASE GIURIDICA** 1. Consenso 2. Contratto	Clienti: aziende e loro dipendenti.	**Dati comuni:** - codice fiscale/partita iva e altri numeri identificativi - attività economiche, commerciali, finanziarie e assicurative - mail - sesso - ruolo ricoperto in azienda	Membri del CDA e Revisori contabili; Studi Professionali per la consulenza; Docenti formatori; Enti di ricerca – ad es. Università; Inail/ISS.	NO	Clienti: periodo di sottoscrizione del CCNL o fino a richiesta di cancellazione.	**STRUMENTI ELETTRONICI** - Password - Back-up - Antivirus - Firewall - Windows aggiornato

FONDAZIONE
RUBES TRIVA
SICUREZZA. LAVORO. AMBIENTE

REGISTRO DEI TRATTAMENTI IN QUALITA' DI RESPONSABILE ESTERNO

SCHEDA REGISTRO DEI TRATTAMENTI
Ultimo aggiornamento 30.09.2019

TITOLARE *OGNI AZIENDA ADERENTE AL CCNL O VOLONTARIA*

TIPOLOGIA DI TRATTAMENTO	FINALITA' E BASE GIURIDICA	CATEGORIE DI INTERESSATI	CATEGORIE DI DATI PERSONALI	CATEGORIE DI DESTINATARI *[indicare eventuali responsabili del trattamento o altri titolari cui i dati siano comunicati]*	TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI *[indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le "garanzie" adottate ai sensi del capo V del RGPD]*	TERMINI ULTIMI DI CANCELLAZIONE PREVISTI	MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE
Registrazione Organizzazione Strutturazione Conservazione Consultazione Elaborazione Selezione **MODALITA':** cartacea ed elettronica	Gestione della formazione dei dipendenti. Programmazione delle attività di consulenza. Utilità sociale **Marketing** Corsi e eventi rilevazione grado di soddisfazione del cliente attraverso test finali anonimi **attività di consulenza** archiviazione nel pubblico interesse, ricerca storica o scientifico fini statistici **BASE GIURIDICA** 1. Consenso 2. Contratto	Dipendenti delle aziende aderenti o volontarie	**Dati comuni:** - codice fiscale e altri numeri identificativi - nome, indirizzo e altri elementi di identificazione personale - istruzione e cultura - dati sul comportamento, profili di utenti, consumatori, contribuenti, ecc. - mail - sesso - ruolo ricoperto in azienda	Membri del CDA e Revisori contabili; Studi Professionali per la consulenza; Docenti formatori; Enti di ricerca – ad es. Università; Inail/ISS.	NO	Clienti: periodo di sottoscrizione del CCNL o fino a richiesta di cancellazione	**MISURE FISICHE** - Armadi chiusi a chiave - Cassaforte - Allarme - Distruggi documenti - Cartelline non leggibili - Contenitori sigillati - Controllo accessi - Estintori **MISURE LOGICHE** - Anonimizzazione **STRUMENTI ELETTRONICI** - Password - Back-up - Antivirus - Firewall - Windows aggiornato

TRATTAMENTI EFFETTUATI

La Scrivente tratta dati relativi a:

- Aziende Clienti

- Fornitori/Consulenti esterni

- Dipendenti

- Candidati Per Rapporti Di Lavoro

Aziende Clienti: i dati trattati sono quelli indispensabili in relazione all'adempimento di obblighi contrattuali o legislativi. La finalità è quella di utilità sociale con base giuridica nell'adesione al CCNL o con adesione volontaria basata sul consenso.

Fornitori: i dati trattati sono quelli indispensabili in relazione all'adempimento di obblighi contrattuali o legislativi. La base giuridica è il contratto di fornitura e la finalità sarà quella di:

- adempimenti in materia fiscale o contabile
- gestione fornitura (docenza, consulenza ecc.)
- obblighi previsti dalla legge
- fatturazione.

Dipendenti: i dati trattati sono quelli necessari all'instaurazione di un rapporto di lavoro. La base giuridica è il contratto di lavoro e la finalità sarà quella relativa a:

- gestione del personale
- adempimenti connessi alle quote di iscrizione ai sindacati
- adempimenti obbligatori in campo fiscale o contabile
- gestione della qualità
- igiene e sicurezza del lavoro
- programmazione attività
- servizi di controllo interno
- trattamento giuridico ed economico.

Sarà probabile entrare in contatto anche con dati sensibili quali ad es. adesione a sindacati, convinzioni religiose, stato di salute, origini razziali ecc. ma ciò sarà possibile perché connesso all'attuazione di adempimenti legislativi o contrattuali.

Candidati per rapporti di lavoro: i dati ricevuti spontaneamente con i CV vengono trattati ed utilizzati solo previa consegna dell'informativa all'interessato. Ogni CV viene conservato solo in presenza dell'autorizzazione al trattamento dati rilasciata dall'interessato.

AMBITI DI TRATTAMENTO DATI

Amministrazione – gestione personale e gestione programmazione attività clienti e fatturazione;

Webmaster – si occupa della gestione delle attività informatiche, compreso il software per la formazione. Quando accede a qualche aspetto informatico tuttavia, gli è totalmente preclusa la possibilità di visualizzare gli utenti.

Consulenti – Casai accede al libretto formativo e si occupa di formazione, Ramazzini invece compie aggiornamenti del sito per quanto riguarda le novità legislative e giurisprudenziali dunque non vede alcun dato personale.

Sito Internet e Marketing – attraverso il sito è possibile inviare newsletter che possono riguardare materiale informativo sulla sicurezza oppure eventi e corsi di formazione. Chi riceve le newsletter ha concesso apposito consenso.

ANALISI DEI RISCHI CHE INCOMBONO SUI DATI
DPIA – VALUTAZIONE DI IMPATTO

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:

- Distruzione di strumentazione da parte di persone malintenzionate.
- Rivelazione di informazioni (da parte del personale o fornitori)
- Uso non autorizzato della strumentazione
- Trattamento (volontario o inconsapevole) non consentito di dati (personali)
- Compromissione di funzioni informatiche
- Errori degli utenti (carenza di consapevolezza, incuria)
- Uso dei servizi da parte di persone non autorizzate
- Uso di servizi in modo non autorizzato
- Furto identità

2. EVENTI RELATIVI AGLI STRUMENTI:

- Perdita di servizi essenziali: Malfunzionamento, indisponibilità e degrado degli strumenti
- Perdita di energia (o sbalzi di tensione)
- Malfunzionamento nei componenti di rete
- Disturbi elettromagnetici
- Virus (malware, anche per mobile)
- Intercettazione (inclusa analisi del traffico)
- Furto di documenti o supporti di memorizzazione
- Furto di apparati o componenti
- Infiltrazione nelle comunicazioni
- Problemi tecnici
- Rischi derivati dal Sito internet
- Malfunzionamenti software applicativi
- Errori di manutenzione hardware e software di base

3. EVENTI RELATIVI AL CONTESTO FISICO-AMBIENTALE:

- Danni fisici: Incendio, Allagamento, Polvere, corrosione, congelamento
- Eventi naturali: Terremoti, Uragani, Fulmini e scariche atmosferiche
- Ingressi non autorizzati
- Accesso non autorizzato alla rete.

Una volta individuati gli eventi potenzialmente dannosi per la sicurezza dei dati verrà valutato l'IMPATTO SULLA SICUREZZA, in relazione a ciascun evento, e la PROBABILITÀ DI ACCADIMENTO. In questo modo emergerà il rischio dell'evento stesso e sarà possibile formulare un primo indicatore omogeneo per i diversi rischi da contrastare.

RISCHIO= IMPATTO x PROBABILITA'

1 – Procedere a classificare l'impatto che l'evento potrebbe avere nella realtà aziendale specifica per i diritti e le libertà degli interessati in una scala da 1 a 11 (1 = Molto Basso, 11 = Molto Alto).

2 – Valutare la probabilità di accadimento nella realtà aziendale specifica in base alle misure di sicurezza in essa applicate, con la stessa scala di valori, da 1 a 11 (1 = Molto Basso, 11 = Molto Alto)

Saremo in grado, in questo modo, di individuare i punti di attenzione su cui focalizzare la nostra analisi e i nostri interventi di sicurezza ed emergerà il rischio effettivo netto cioè ridotto sulla base delle contromisure adottate in azienda.

In base alle misure di sicurezza applicate e ai controlli eseguiti nel trattamento, esposti a seguire, andremo a ridurre sempre di più la probabilità/frequenza di accadimento e/o l'impatto per le varie tipologie di rischio analizzate.

La riduzione del livello di rischio, dal rischio generico al rischio effettivo, rappresenta l'efficacia delle misure di sicurezza applicate e dovrebbe evidenziare gli interventi/investimenti fatti per assicurare la "sicurezza".

Le misure di sicurezza applicate devono essere: efficaci, effettive, monitorate e controllate periodicamente, valutate in modo oggettivo, mantenendo evidenze dell'attività eseguita.

Rating per la classificazione del livello di rischio

Quando la valutazione del "rischio netto" nella matrice è:

verde ($p*i < 7$) = livello di rischio considerato accettabile;

giallo ($p*i < 11$) = necessario pianificare interventi di mitigazione;

arancio/rosso ($p*i > 11$) = indispensabile attivare rapidamente contromisure di adeguamento.

Rischio	Linee guida per la valutazione
1 - Basso	È applicabile ad almeno uno dei seguenti: - la minaccia è raro che si verifichi; - in caso di **attacco**, i dati sono poco appetibili e l'immagine aziendale non è compromessa e pertanto i tentativi di attacco o non sono iniziati o sono condotti da malintenzionati scarsamente preparati da un punto di vista tecnico e con scarse risorse a disposizione. - in caso di **eventi naturali**, gli studi dimostrano che la minaccia può verificarsi molto raramente.
2 - Medio	È applicabile ad almeno uno dei seguenti: - la minaccia si può verificare; - in caso di **attacco**, i dati sono poco appetibili e l'immagine aziendale può non essere del tutto compromessa; - in caso di **eventi naturali**, gli studi dimostrano che la minaccia può verificarsi nella media dei casi studiati.
3 - Alto	È applicabile ad almeno uno dei seguenti: - la minaccia si può verificare più frequentemente rispetto alle altre due casistiche; - in caso di **attacco**, i dati sono appetibili o l'immagine aziendale è compromessa; - in caso di **eventi naturali**, gli studi dimostrano che la minaccia si verifica quasi certamente.

COMPORTAMENTO DEGLI OPERATORI			
EVENTO	**IMPATTO**	**PROBABILITA' DI ACCADIMENTO**	**RISCHIO**
Distruzione di strumentazione da parte di persone malintenzionate.	2	2	BASSO
Rivelazione di informazioni (da parte del personale o fornitori)	2	2	BASSO
Uso non autorizzato della strumentazione	2	2	BASSO
Trattamento (volontario o inconsapevole) non consentito di dati (personali)	1	1	BASSO
Compromissione di funzioni informatiche	3	2	BASSO
Errori degli utenti (carenza di consapevolezza, incuria)	1	3	BASSO
Uso dei servizi da parte di persone non autorizzate	1	2	BASSO
Uso di servizi in modo non autorizzato	1	2	BASSO
Furto identità	2	2	BASSO

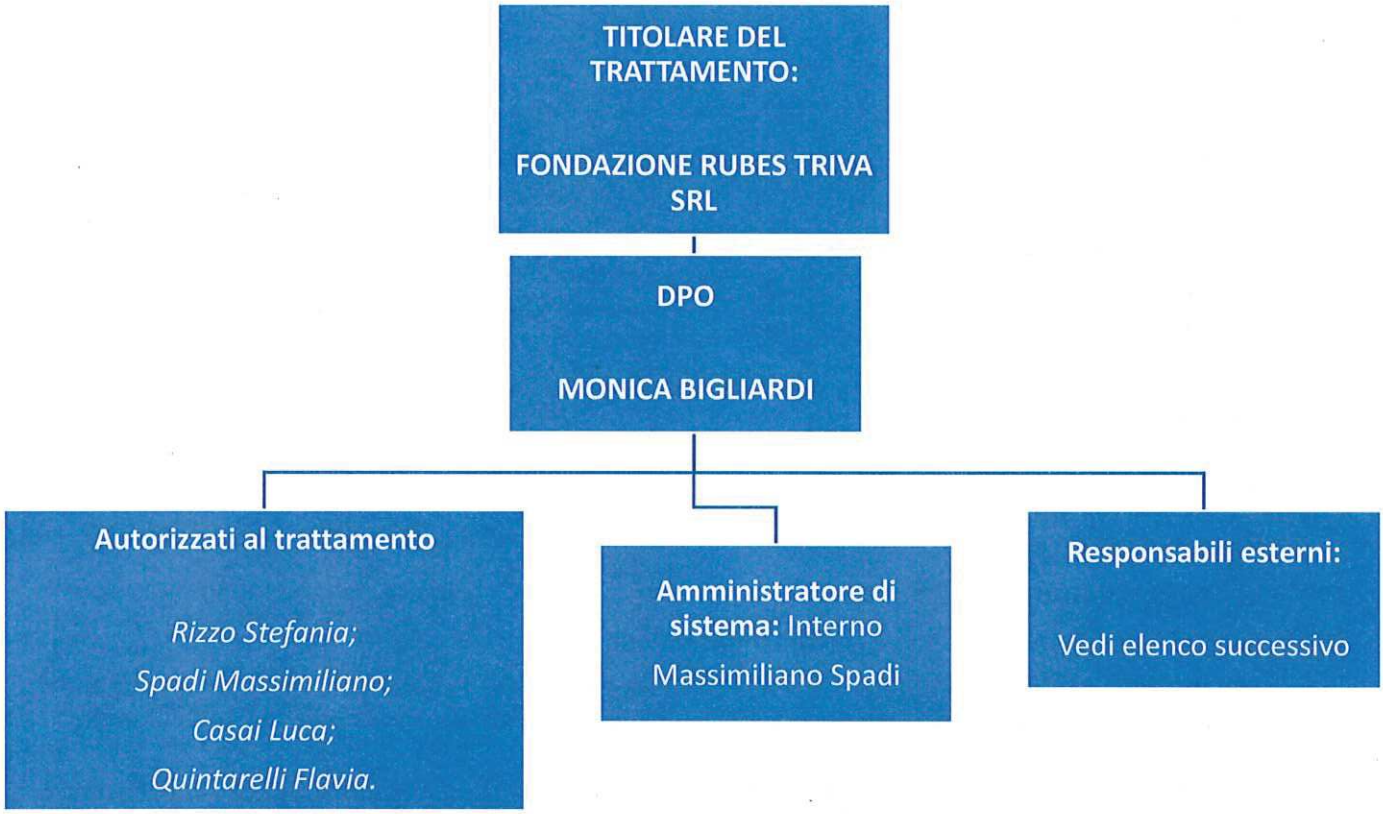
EVENTI RELATIVI AGLI STRUMENTI			
EVENTO	**IMPATTO**	**PROBABILITA' DI ACCADIMENTO**	**RISCHIO**
Perdita di servizi essenziali: Malfunzionamento, indisponibilità e degrado degli strumenti	2	1	BASSO
Perdita di energia (o sbalzi di tensione)	1	2	BASSO
Malfunzionamento nei componenti di rete	1	2	BASSO
Disturbi elettromagnetici	1	2	BASSO
Virus (malware, anche per mobile)	3	2	BASSO
Intercettazione (inclusa analisi del traffico)	2	2	BASSO
Furto di documenti o supporti di memorizzazione	1	2	BASSO
Furto di apparati o componenti	1	2	BASSO
Infiltrazione nelle comunicazioni	2	2	BASSO
Problemi tecnici	1	2	BASSO
Rischi derivati dal Sito internet	1	2	BASSO
Malfunzionamenti software applicativi	2	2	BASSO
Errori di manutenzione hardware e software di base	2	2	BASSO

EVENTI RELATIVI AL CONTESTO FISICO-AMBIENTALE			
EVENTO	**IMPATTO**	**PROBABILITA' DI ACCADIMENTO**	**RISCHIO**
Danni fisici: Incendio, Allagamento, Polvere, corrosione, congelamento	2	3	BASSO
Eventi naturali: Terremoti, Uragani, Fulmini e scariche atmosferiche	3	2	BASSO
Ingressi non autorizzati	2	1	BASSO
Accesso non autorizzato alla rete.	3	1	BASSO

Per tutte le categorie in cui il valore sia superiore a 7, quindi in fascia Gialla e Rossa, è necessario adottare le misure di miglioramento indicate nella tabella predisposta a fine documento al fine di ridurre il rischio.

In fascia rossa non è più presente alcun evento poiché l'azienda si è dotata di numerose migliorie, soprattutto in ambito informatico.

ORGANIGRAMMA AZIENDALE



L'amministratore di sistema viene nominato con apposito incarico e viene monitorato ogni anno con una valutazione annuale del suo operato per continuare a verificare che tale nomina sia appropriata.

ORGANIGRAMMA

PRESIDENTE
Francesco Iacotucci

DIRETTORE
Giuseppe Mulazzi

FONDAZIONE
RUBES TRIVA
SICUREZZA, LAVORO, AMBIENTE

CONSIGLIO DI AMMINISTRAZIONE
Annamaria Caputi
Massimo Cenciotti
Paolo Collini
Nedo Domizi
Paolo Giacomelli
Valentina Pinori
Luigi Verzicco

COLLEGIO DEI REVISORI DEI CONTI
Presidente
Vincenzo Pagnozzi

Revisori
Giovanni Pizzolla
Vito Rosati

DPO
Bigliardi Monica nella sua qualità di dipendente

Con apposito verbale di riunione del CDA, è stato nominato il Direttore Giuseppe Mulazzi come persona fisica di riferimento per tutto ciò che riguarda l'adempimento degli obblighi in materia di privacy.
I membri del CDA hanno unanimamente approvato la documentazione nei consigli tenutisi il 07/06/2017 e 22/03/2018.

STRUTTURA ORGANICA

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

Formazione e Libretto Formativo
Flavia Quintarelli
Tel: 06 32 690 411 Fax: 06 32 22 595
mail:
quintarelli@fondazionerubestriva.it

RESPONSABILI ESTERNI:

Centro Antinfortunistico srl – S.U. per gestione adempimenti privacy e consulenza sicurezza sul lavoro

Galusi Tiziano – contabilità

Stucchi & Stucchi S.r.l. – Consulente del lavoro

Banche

Assicurazioni

Inail

Istituti Universitari

Enti Fiere: Ecomondo e Ambiente e Lavoro

Docenti

DIFFUSIONE DATI

La Società con compie alcuna diffusione dei dati personali a mezzo stampa, internet, radio ecc.

BANCHE DATI E SOFTWARE GESTIONALI

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 di Tiziano Galusi, nominato Responsabile esterno del trattamento.

La Fondazione accede direttamente al software di Galusi e si connette mediante credenziali per inserire i documenti utili alla contabilità.

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

Alla luce dei rischi individuati, la Società 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 Società innanzitutto tratta i dati rispettando i principi esplicitamente indicati nell'art. 5 del Reg. 2016/679 – come sopra esplicitato - 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** a disposizione dell'azienda anteriormente al trattamento del dato stesso. La Fondazione entra infatti in contatto con i dati aziendali – soprattutto dei dipendenti – solo al momento della compilazione del gestionale da parte dell'azienda stessa.

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 mette a disposizione del cliente l'informativa privacy da visualizzare per poter procedere con l'inserimento dei dati. Sarà il responsabile aziendale appositamente nominato a prestare il consenso e ad avere pieno 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.

Ogni dipendente e/o collaboratore è stato nominato autorizzato al trattamento dati attraverso apposito incarico di cui all'**Allegato E** e relative istruzioni.

I dipendenti della Fondazione hanno frequentato apposito corso di formazione in materia di privacy nella giornata del 02 maggio 2018 e un aggiornamento nella giornata del 26.09.2019.

DATA BREACH

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, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui se ne viene a conoscenza.

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

La Fondazione ha previsto - all'interno dell'incarico al trattamento dati dei dipendenti - apposito obbligo di segnalazione immediata al DPO di eventuali violazioni in materia di tutela dei dati personali. Il legale rappresentante ha poi a disposizione il modulo di comunicazione reso noto dal Garante Privacy al link https://www.garanteprivacy.it/documents/10160/0/Modello+notifica+Data+Breach.pdf/6d1fa433-88dc-2711-22ab-dd5d476abe74?version=1.1: sarà necessario scaricarlo e compilarlo.

PROCEDURA:

Rilevazione e analisi dei rischi del Data Breach

1. Rilevare e accertarsi della violazione
2. Avviare l'azione correttiva per gestire tecnicamente il **Data Breach**
3. Analizzare la violazione e valutarne i rischi connessi

Data Breach: assenza di rischi

In caso non ci fosse alcun rischio connesso all'attacco verso i dati personali immagazzinati, è necessario registrare la violazione e successivamente conservare il registro. La notifica al Garante della Privacy non è obbligatoria ed è comunque necessario comprovare l'assenza dei rischi.

Data Breach: presenza di rischi

In presenza di rischi per gli interessati è necessaria la **notifica, senza ritardo e comunque entro 72 ore** al **Garante della Privacy**.

1. Raccogliere tutte le informazioni inerenti al **Data Breach** per la notifica al **Garante della Privacy**
2. Inviare la notifica al **Garante della Privacy scaricando il modulo sopra indicato**
3. Registrare la violazione
4. Conservare il registro delle violazioni

I principali rischi connessi a un Data Breach

- danni fisici, materiali o immateriali alle persone fisiche
- perdita del controllo dei dati personali
- limitazione dei diritti, discriminazione
- furto di identità
- perdite finanziarie, danno economico o sociale
- decifratura non autorizzata della pseudonimizzazione
- pregiudizio alla reputazione
- perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari)

Data Breach: presenza di un elevato rischio

1. Raccogliere tutte le informazioni inerenti al **Data Breach** per la notifica al **Garante della Privacy** e ai diretti interessati del trattamento
2. Inviare la notifica al **Garante della Privacy** e agli interessati
3. Gestione dei riscontri da parte degli interessati
4. Registrare la violazione
5. Conservare il registro delle violazioni

Per un rischio elevato si intende per esempio una violazione che interessa un un rilevante quantitativo di dati personali e/o di soggetti interessati, piuttosto che un **Data Breach** che impatta su soggetti vulnerabili per le loro condizioni o categorie particolari di dati personali.

La segnalazione deve essere effettuata dal Titolare del Trattamento.

Notifica di Data breach: La notifica deve essere inviata al Garante tramite posta elettronica all'indirizzo protocollo@pec.gpdp.it e deve essere sottoscritta digitalmente (con firma elettronica qualificata/firma digitale) ovvero con firma autografa. In quest'ultimo caso la notifica deve essere presentata unitamente alla copia del documento d'identità del firmatario.

L'oggetto del messaggio deve contenere obbligatoriamente la dicitura "NOTIFICA VIOLAZIONE DATI PERSONALI" e opzionalmente la denominazione del titolare del trattamento.

LE AZIONI DEL GARANTE

Il Garante può prescrivere misure correttive (v. art. 58, paragrafo 2, del Regolamento UE 2016/679) nel caso sia rilevata una violazione delle disposizioni del Regolamento stesso, anche per quanto riguarda l'adeguatezza delle misure di sicurezza tecniche e organizzative applicate ai dati oggetto di violazione. Sono previste sanzioni pecuniarie che possono arrivare fino a 10 milioni di Euro o, nel caso di imprese, fino al 2% del fatturato totale annuo mondiale.

TRASFERIMENTO DATI ALL'ESTERO

La Società non trasferisce i dati all'estero

DIRITTI DELL'INTERESSATO

Alla luce degli articoli 15 e ss. Del Regolamento, vari sono i diritti dell'interessato e si 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);**
- **Diritto di proporre reclamo all'Autorità di controllo.**

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

Esiste una segreteria telefonica senza possibilità di registrazione del messaggio.

DATI CARTACEI

Attualmente l'archivio dei documenti si trova all'interno degli uffici e vengono sempre chiusi a chiave.

Inoltre:

- E' presente un distruggi documenti;
- Qualsiasi documento contenente dati personali in entrata/uscita viene inserito in apposite cartelline non trasparenti, raccoglitori o buste;
- L'ubicazione di stampanti ed apparecchio fax tradizionale non consente ad estranei di leggere od asportare eventualmente documenti; le aree contenenti stampanti ed apparecchio fax sono ubicate 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.

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

•Le copie dei fax inviati e ricevuti vengono archiviati in appositi raccoglitori che successivamente verranno archiviati in armadi;

•Nella pagine accompagnatoria dei Fax viene digitata la seguente dicitura: *"in ottemperanza al Reg. UE 2016/679 e al D. Lgs. 196/2003 – così come modificato dal d.lgs. 101/2018 - le informazioni contenute in questo fax sono destinate esclusivamente agli individui e agli enti ai quali risulta indirizzato. 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. Gli indirizzi nel nostro archivio provengono da richieste pervenute alla nostra Società. In ogni momento è possibile avere accesso, modificare, limitare o cancellare i dati presenti nei nostri archivi inviando un fax al numero 063222595. L'informativa completa è disponibile presso i nostri uffici."*.

•Tutti gli archivi cartacei relativi ai dipendenti sono chiusi all'interno di raccoglitori inseriti in un apposito armadio nell'ufficio che a fine orario di lavoro viene sempre chiuso a chiave.

DATI ELETTRONICI

La Società dispone di un sito internet curato internamente dal webmaster.
Nel sito è prevista una informativa e una cookie policy.
Sono presenti 5 PC fissi.

- I dati di tipo informatico vengono protetti tramite l'utilizzo di passwords: le passwords sono costituite da 8 caratteri alfanumerici e vengono cambiate 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.
  Monica Bigliardi accede ai dati relativi alla segreteria e alla contabilità;
  Stefania Rizzo accede ai dati relativi alla segreteria e alla contabilità;
  Massimiliano Spadi accede ai dati informatici.
- I computer risultano tutti sollevati da terra in modo da evitare perdite di dati in caso di eventi improvvisi come un allagamento;
- È presente una rete di ufficio e una VPN per il collegamento in remoto.
- Tutta l'amministrazione lavora direttamente nel server.
- L'integrità dei dati è inoltre garantita mediante idonee procedure di salvataggio periodico (backup): il backup viene fatto sia sul server sia su altri due supporti, uno in un hard disk del pc e un'altra copia in altro hard disk. Le copie dei back up sono appositamente conservate all'interno di una cassaforte ignifuga.
- Ad oggi avviene anche un terzo salvataggio su Cloud– Google.
- 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.
- In merito a messaggi e-mail inviati a più destinatari, quale mittente viene indicato 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);
- Le penne usb contenenti dati dei clienti vengono riutilizzate esclusivamente previa formattazione irreversibile, in modo da impedire la letture dei dati precedenti e dotandole di un proprio codice di accesso.
- Tutti i giorni, in orario di chiusura, i pc vanno in modalità stand-by. Dunque per la riattivazione è necessaria la password.
- 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;
- È presente un Firewall.

FONDAZIONE
RUBES TRIVA
SICUREZZA. LAVORO. AMBIENTE

PROGRAMMA DI MIGLIORAMENTO

Intervento	Priorità	Da Attuarsi Entro	Responsabile dell'attuazione	Data di attuazione
Analisi e valutazione continua e sistematica delle misure adottate	Media	Da attuarsi costantemente	_____	Firma _____
Valutazione dell'applicazione del nuovo Regolamento europeo e adeguamento ai provvedimenti del Garante Privacy	Media	Da attuarsi costantemente	_____	
Responsabilizzazione massima di tutti gli operatori anche tramite interventi formativi ed informativi	Media	Organizzazione periodica del Titolare del trattamento	_____	
Cambio automatico delle password dei pc con sistema automatizzato da installare nel pc	Alta	Immediatamente	_____	
Conservare il codice della licenza di acquisto dell'antivirus	Alta	Immediatamente	_____	
Implementare le misure di sicurezza dei sistemi informatici attraverso l'analisi delle misure più opportune indicate dal consulente informatico	Alta	Immediatamente	_____	
Predisporre una mappatura dei sistemi informatici e delle banche dati insieme al proprio consulente informatico	Alta	Immediatamente	_____	
Verificare che in fondo alla mail, anche inviata via telefono, sia inserita la dicitura: "in ottemperanza al Reg. UE 2016/679 e al D. Lgs. 196/2003 – come modificato dal d. Lgs. 101/2018 - le informazioni contenute in questa mail sono destinate esclusivamente agli individui e agli enti ai quali risulta indirizzato. Se Lei non è tra i destinatari originari non deve utilizzare, rivelare, trasmettere, copiare né stampare il suo contenuto. Se Lei ha ricevuto questa mail per errore, è pregato di avvisarci e quindi distruggere il documento. Gli indirizzi e-mail nel nostro archivio provengono da contratti in essere o da richieste pervenute alla nostra Fondazione. Il Titolare del Trattamento è Fondazione Nazionale Sicurezza Rubes Triva. In ogni momento è possibile avere accesso, modificare, limitare o cancellare i dati presenti nei nostri archivi inviando una mail all'indirizzo mulazzi@fondazionerubestriva.it . L'informativa completa è disponibile presso i nostri uffici".	Media	Immediatamente	_____	

Effettuare penetration test periodici	Alta	Periodicamente	_____ _____	
Dotarsi di un sistema di crittografia/pseudonimizzazione o almeno anonimizzazione	Alta	Immediatamente	_____ _____	
Verificare che il sito rispetti le normative sui cookies e sulla parte dei contatti	Alta	Immediatamente	_____ _____	
Dotarsi di **misure fisiche** adeguate: armadi ignifughi	Alta	Immediatamente	Titolare del Trattamento	
Aggiungere – se non ha già provveduto il gestore della segreteria telefonica – un messaggio breve di informativa sul trattamento dati del chiamante.	Media	Quanto prima	Titolare del trattamento	

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 per qualsiasi dipendente o collaboratore voglia consultarlo e ognuno è tenuto, in base ai propri incarichi, al suo pieno rispetto.

IL TITOLARE DEL TRATTAMENTO

Firma e timbro aziendale

Fondazione Nazionale Sicurezza
"Rubes Triva"
Il Direttore
(Giuseppe Mularzi)