DOCUMENTAZIONE DI SISTEMA PER IL TRATTAMENTO DELLE INFORMAZIONI PERSONALI

MANUALE SISTEMA PRIVACY E DATA PROTECTION
EDIZIONE (Anno 2016-17)

Dichiarazione ai sensi degli Art. 30 del Regolamento 679/2016 ratifica Maggio 2016

La Società detiene un Manuale del Sistema Privacy con l'attivo aggiornamento delle misure idonee di tutela delle informazioni personali in conformità alle prescrizioni di legge in accordo al recepimento delle nuove direttive Europee sul Data Protection GDPR (già Regolamento 2016/679) ratificate il 14 Maggio 2016 (vedi ***DTT1/4***). Suddetto regolamento prevede la redazione del presente

PRE-ASSESSMENT PER MIGRAZIONE AL REGISTRO DEI TRATTAMENTI

Sigla Documento : **RTP2016** (Def. MDPS/196)
Prima Versione : **1.0 – Sett 2016**
Aggiornamento : **previsto Marzo 2017**
Ultima revisione : **1.0 – Sett 2016 da Audit interno Agosto 2016**

Indice del Registro dei Trattamenti

Nome e dati di contatto del titolare del trattamento e contitolare del trattamento e del responsabile della protezione dei dati	**A) Ver. 1.1**
Finalità del trattamento	**B) Ver. 1.0**
Categorie di interessati e delle categorie di dati personali	**C) Ver. 2.1**
Categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali	**D) Ver. 1.0**
Trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate	**N.A.**
Termini ultimi previsti per la cancellazione delle diverse categorie di dati	**F) Ver. 1.4bis**
Descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.	**G) Ver. 1.5**

Nel suo insieme la collezione di registrazioni, documenti e deleghe costituisce il Manuale del Sistema Privacy e pertiene Trattamenti sia automatizzati che cartacei.

Come prescritto dal Disciplinare Interno della Azienda e dall'Art. 30 co.3 del Reg.679/2016 , tutti i documenti sono resi disponibili anche attraverso formato elettronico su CMS INTRALAN per la conoscenza dei lavoratori/dipendenti e/o stagisti afferenti alle aree di trattamenti di cui sopra.

Il Titolare dei dati /
Data Controller
R&S MANAGEMENT S.r.l.
l'amministratore unico
Dott.ssa Serena Borelli
.....

Tutti i documenti e le registrazioni della documentazione e i loro aggiornamenti sono redatti, revisionati e approvati dal Titolare del Trattamento dei Dati della Società o dal persone delegate nelle rispettive competenze. Tutte le edizioni di documenti per il quale è prevista l'archiviazione avviene in aree sicure ad accesso controllato. Anche i Soggetti Privacy Designati delocalizzati ricevono copia dell presente documento oltre alle procedure di propria competenza.

A) Ver. 1.1 - Nome e dati di contatto del titolare del trattamento e contitolare del trattamento e del responsabile della protezione dei dati

Titolare del trattamento:

R&S Management S.r.l.
C. Fisc. e N. Iscr. Reg. 07828660584 – P.IVA 01458820766– REA RM 975777 – Cap. Soc. 1.600.000,00 Euro
www. rsmanagement.it - E-mail info@rsmanagement.it - resmanagement@certificazioneposta.it
Sede Legale e Direzione: V.lo delle Siepi, 2 – 00072 Ariccia (RM) – Tel. 06.9344940 – Fax 06.94805307
Altra Unità Operativa: Via Chiusa, 11 - 84046 Ascea (SA) 334 6009378

Organismo accreditato ACCREDIA
CSQA
UNI EN ISO 9001:2015
SGQ Cerificato n°

Contitolare del Trattamento:

SEFT s.r.l. Sistemi per l'elaborazione la formazione e tecniche direzionali
Capitale Sociale Euro. 50.000,00 i.v. Iscr. Trib. Velletri 3544 CCIAA 490674
P.IVA 01390691002 C.F. 05342110581
Vicolo delle Siepi, 2 – 00072 Ariccia (RM) ☎ 06/9342051-9344940 FAX 06/94805307 - seft@pec.it

Responsabile del Trattamento (delega dove presente DPO indipendente):

Dott.ssa Sara Borelli

Responsabile coordinatore interno del Trattamento:
Dott.ssa Sara Borelli

B) Ver. 1.0 - Finalità del trattamento

Descrizione generale: **La finalità di tutti i trattamenti è quella di garantire alla clientela il miglior progetto realizzativo e il miglior servizio di manutenzione impiantistico possibile dei Sistemi di Elevazione della Azienda.**

Tipologie di finalità: **La prima finalità di carattere anagrafico de trattamenti è mirata alla soddisfazione del cliente (sia esso noto o nuovo) per ciò che attiene il rapporto di fornitura. In seconda istanza, e per quei clienti che instaurano un rapporto consolidato nel tempo ai fini di garanzia manutentiva, i dati raccolti sono necessari alla messa in atto di un accordo di Polizza manutentiva per la certezza di interventi nel tempo in occasione di emergenze, malfunzionamenti o semplicemente monitoraggi degli impianti presso cliente.**

C) Ver. 2.1 - Categorie di interessati e delle categorie di dati personali

Durante le fasi precoci di pre-assessment e audit interno al sistema non sono stati identificate categorie di destinatari diversi dai soggetti gestiti nel sistema automatizzato ERP/CRM della Azienda nell'ambito delle attività commerciali di business.

D) Ver. 1.0 - Categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali

Vedi Punto C)

E) N.A. - Trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresal'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate

Non Applicabile

F) Ver. 1.4bis - Termini ultimi previsti per la cancellazione delle diverse categorie di dati

Tutti i dati e le informazioni trattate all'interno del campo di definizione e applicazione del Regolamento 679/2016 Artt. 29, 30 e 32 sono detenuti secondo il seguente schema:

Contenuti su supporto cartaceo
La RS&Management Srl intraprende la Dematerializzazione/Rilocazione sicura/distruzione con cadenza di 10-15 anni nel rispetto delle normative in materia di Tributaria e Amministrazione delle Fiscalità.

Contenuti su supporto informatico
La RS&Management Srl segue un Piano di Adeguamento tecnologico in accordo al quale le misure idonee di cui all' Art. 33 del GDPR-2016-EU.

Tutti i supporti informatici di stoccaggio delle informazioni sono ridondate con tecnologia RAID di livello 5 (striping con parità). Lo stoccaggio dei dati viene realizzato sia sotto forma di immagini digitali con hashing forenze (MD5,SHA256) per i contenuti detenuti dentro i data base, sia sotto forma di volumi compressi e cifrati per ciò che attiene i files distribuiti nei vari file system della rete interna (INTRALAN).

Pertanto, in ragione dei supporti sopra citati, la cancellazione viene calendarizzata in modo automatico ma comunque supervisionato su base annuale a mezzo di Gestione di un sistema di monitoraggio che trasmette comunicazioni a mezzo email e sms al DPO, al responsabile di coordinamento e alla Proprietà nella persona del legale rappresentante del Titolare del Trattamento.

Tali attività permagono comunque registrate negli annali di backup storicizzati sotto algoritmo di cifratura.

Quanto elettronicamente mantenuto e persistito su media ottici, viene reso intellegibile solamente alle Forze di Polizia e/o della Autorità Costituita in adempimento alle norme di Data Retention (ex lege Pisanu).

G) Ver. 1.5 - Descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32,paragrafo 1.

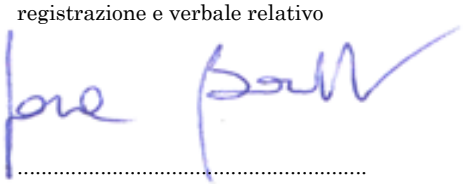
La RS&Management Srl e il proprio Contitolare di cui al punto A), distinguono i seguenti livelli di misure tecniche ed organizzative legate al trattamento delle informazioni e quindi dei dati personali di cui al Reg.679/2016

1) **Resilienza della infrastruttura informatica – Gestione Logs/GPO/accountability**
2) **Procedure e istruzioni operative di confidenzialità dei contenuti cartacei**
3) **Aggiornamenti e *appliance* di HW e SW utilizzato a livello Sistema e Applicativo**
4) **Policy su apparati anti-intrusione e architettura perimetrale (DMZ/services/Subnet)**
5) **Politiche di redirezione e instradamento delle trasmissioni tramite tecniche di controllo sul livello protocolli di comunicazione a mezzo DHCP/Mac, NAT e PAT a monte del flusso LAN su apparato dedicato ROUTER/Firewall**
6) **Segregazione ambito di connettività fonia e dati (VOIP versus HDSL)**
7) **Formazione operatori (data processors) e affiancamento ADS sulle diligenze dovute e sulle prassi corrette di utilizzo di tutte le stazioni di lavorio su Dominio Active Directory MS Windows Server. Monitoraggio ACS fuori Orario e connessioni WAN-to-LAN. Divulgazione del Disciplinare Interno IT**
8) **Utilizzo di cifratura con certificato proprietario sia per protocolli di comunicazione che per non-repudiabilità. Per i contenuti nei volumi distribuiti e/o condivisi sono usate chiavi uni-direzionali proprietarie. Volumi digitalmente machiati con hasching sha256 sono quindi stoccati nelle periferiche NAS**
9) **Accordi transattivi SLA e PLA per la riqualifica delle forniture ICT**
10) **Serramenti e vetrofanie di difesa passiva per gli ambienti del CED**

Dettagli delle procedure e della prassi operative e attuative sono consultabili nelle verbalizzazioni registrate nel Manuale del Sistema di Data Protection aziendale (MSDPA) detenuto presso i Coordinatori sia nella sede di Milano che in quella del Contitolare di Torino.

L'indice del MSDPA segue questo documento nel faldone classificato presso gli uffici. Su richiesta nell'armadio ARM1 sono disponibili copie coonformi die documenti di nomina/delega della fidure e die soggetti del SDPA e della Gestione delle credenziali per il controllo ACL di tutta la infrastruttura informatica.

Alla data della
registrazione e verbale relativo



.....