AZIENDA MULTISERVIZI VALENZANA S.P.A.

CERTIFICATA CON SISTEMA DI QUALITA'
SECONDO LE NORME UNI EN ISO 9001:2008
SERVIZIO IDRICO INTEGRATO

Prot. n° 274 Valenza, 25 maggio 2018

PROCEDURE PER L'ADEGUAMENTO ED IL RISPETTO DELLE NORME PREVISTE DAL REGOLAMENTO UE 2016/679 (Regolamento generale sulla protezione dei dati)

PREMESSA

Il presente documento è redatto in coerenza al D.Lgs 196/2003 "Codice in materia di protezione dei dati personali", al Regolamento UE 2016/679 (Regolamento generale sulla protezione dei dati).
Lo stesso costituisce integrazione al modello ex D lgs 231/2001 adottato dalla società ed al vigente regolamento aziendale.
AMV spa nell'ambito del costituito Raggruppamento Temporaneo di Impresa - Servizio idrico Integrato - con AMC spa di Casale M.to nel mese di febbraio 2018 ha sottoscritto specifico contratto per la fornitura di servizi software al fine di addivenire ad un ottimale implementazione del sistema gestionale che entrerà a regime entro il mese di ottobre 2018. AMC mediante la Società fornitrice del software ha previsto nei tempi tecnici necessari, un adeguamento al Regolamento UE 2016-676 in materia di protezione dei dati dei prodotti software specificatamente utilizzati denominati Net@SIAL e Net@H2O.
Scopo di questo documento è di delineare il quadro delle misure di sicurezza, organizzative, fisiche e logiche, adottate per il trattamento dei dati personali, identificativi, sensibili e giudiziari effettuato da parte di AMV spa, in persona dell'amministratore unico e legale rappresentate pro tempore.

Nel presente documento si forniscono idonee informazioni riguardanti:

1. l'elenco dei trattamenti di dati personali, mediante:
   - l'individuazione dei tipi di dati personali trattati.
   - la descrizione delle aree, dei locali e degli strumenti con i quali si effettuano i trattamenti.
   - l'indicazione delle finalità per cui vengono trattati i dati.
2. il nominativo e i dati di contatto del titolare del trattamento, nonché la distribuzione dei compiti e delle responsabilità, nell'ambito delle strutture preposte al trattamento dei dati e previsione di interventi formativi degli incaricati del trattamento.
3. l'analisi dei rischi che incombono sui dati, nonché le misure, già adottate e da adottare, per garantire l'integrità e la disponibilità dei dati; i criteri e le modalità di ripristino dei dati, in seguito a distruzione o danneggiamento i criteri da adottare, per garantire l'adozione delle misure minime di sicurezza, in caso di trattamenti di dati personali affidati all'esterno.
4. Considerazioni conclusive e conseguenze applicative.
5. Dichiarazione d'impegno e firma.

Indice

1. Elenco dei trattamenti dei dati personali

1.1 Tipologie di dati trattati

I dati trattati dal Titolare risultano essere esclusivamente quelli necessari all'assolvimento delle funzioni ed attività connesse ai servizi gestiti da AMV spa (servizio idrico integrato e sosta), ovvero quelli trattati nell'ambito del rapporto di lavoro instaurato con personale dipendente all'interno dell'azienda, ovvero con collaboratori, consulenti esterni, con società per contratti di servizio.
L'insieme della tipologia dei dati trattati ricomprende pertanto i seguenti dati comuni, sensibili e giudiziari relativi a clienti-utenti/ fornitori / personale / candidati per l'instaurazione di rapporti di lavoro / collaboratori / consulenti e professionisti esterni:

- dati comuni dei clienti-utenti, dei fornitori e di terzi ricavati da albi, elenchi pubblici, visure camerali e di fonti analoghe;
- dati comuni del personale dipendente necessari al rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi, dati richiesti ai fini fiscali, previdenziali, e di natura bancaria e postale;
- dati comuni dei clienti-utenti , dagli stessi forniti nell'ambito dei servizi pubblici gestiti, oltre a quelli afferenti alla reperibilità ed alla corrispondenza con gli stessi, di natura bancaria e postale;
- dati comuni dei fornitori concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti ai fini fiscali e dati di natura bancaria e postale;
- dati comuni di professionisti ai quali AMV spa si rivolge per servizi e consulenze , quali quelli concernenti la reperibilità e la corrispondenza con gli stessi, inerenti a finalità fiscali, di natura bancaria e postale;
- dati sensibili e giudiziari del personale dipendente, conseguenti al rapporto di lavoro e inerenti i rapporti con gli enti previdenziali ed assistenziali;
- dati sensibili e giudiziari dei candidati per l'instaurazione di un rapporto di lavoro.

1.2 Caratteristiche di aree, locali e strumenti con cui si effettuano i trattamenti

Uffici

Il trattamento dei dati personali avviene di norma presso gli uffici della sede di AMV spa in Valenza, Strada Pontecurone, 1.
L'accesso alla sede è consentito ai clienti-utenti secondo gli orari di apertura al pubblico regolamentati ed adeguatamente pubblicizzati. Tale accesso consta di un meccanismo automatico.
Il personale dipendente è munito di chiavi, il servizio di centralino è presidiato dall'ufficio back office.
Le finestre della struttura sono protette da imposte in alluminio, dotate ciascuna di idoneo sistema di blocco meccanico interno atto ad impedire l'apertura dall'esterno una volta chiuse durante gli orari ed i giorni in cui gli uffici non sono presidiati.
I due locali destinati ad archivio posizionati al piano terra ed al primo piano risultano chiusi con idonea serratura a chiave.
Di quello al piano terra sono in possesso di relative chiavi conservate in idonea cassetta di sicurezza gli uffici: Affari Generali e Personale.
Di quello al piano superiore sono in possesso di relative chiavi gli uffici: Personale e Contabilità.
La sede aziendale è dotata di idoneo sistema di allarme.

Il trattamento dei dati personali avviene con i **seguenti strumenti**:

A – Schedari ed altri supporti cartacei

I supporti cartacei, ed altri supporti idonei a conservare dati personali, ivi inclusi quelli contenenti suoni od immagini, vengono ordinatamente raccolti in schedari/faldoni, ovvero nella pratica cui si riferiscono, per essere archiviati all'interno di armadi ciascuno dotato di chiusura a chiave.

B – Elaboratori in rete pubblica

L'accesso alla rete aziendale è regolata da password di identificazione. I PC connessi in rete dispongono di collegamento ad Internet.

2. Mansionario privacy ed interventi formativi degli incaricati

Titolare del trattamento è AMV spa nella persona del legale rappresentante, società a totale partecipazione pubblica, il cui socio maggioritario è rappresentato dal Comune di Valenza. L'organo amministrativo è in coerenza a quanto stabilito dall'Assemblea Soci è monocratico.
L'amministratore unico ha proceduto alla nomina degli **Incaricati del trattamento - IdT.**
L'Atto di nomina costituisce parte integrante del presente documento e per tale motivo allegato.

Consulente esterno incaricato dell'assistenza e manutenzione degli strumenti elettronici è la società SEC di Zelaschi & C di Tortona (AL).

I dati, così come schematizzati nel paragrafo precedente, sono trattati da tutti gli incaricati **che hanno ricevuto un formale incarico**, mediante specifica designazione scritta.
Oltre alle istruzioni generali su come devono essere trattati i dati personali, agli incaricati vengono fornite esplicite istruzioni in merito ai seguenti punti, ciò al fine di garantire la sicurezza del trattamento medesimo:

- procedure da seguire per la classificazione dei dati, al fine di distinguere quelli sensibili e giudiziari, per garantire la sicurezza dei quali occorrono maggiori cautele, rispetto a quanto è previsto per i dati di natura comune

- modalità di reperimento dei documenti, contenenti dati personali, e modalità da osservare per la custodia degli stessi e la loro archiviazione, al termine dello svolgimento del lavoro per il quale è stato necessario utilizzare i documenti
- modalità per elaborare e custodire le *password*, necessarie per accedere ai PC ed ai dati in essi contenuti, nonché per fornirne una copia all'amministratore di sistema o a persona dallo stesso designata alla custodia delle parole chiave
- prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici, mentre è in corso una sessione di lavoro
- procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi
- procedure per il salvataggio dei dati
- modalità di custodia ed utilizzo dei supporti rimuovibili, contenenti dati personali
- dovere di aggiornarsi, utilizzando il materiale e gli strumenti forniti dal Titolare, sulle misure di sicurezza.

Al/i soggetto/i incaricato/i della gestione e manutenzione del sistema informativo viene prescritto di non effettuare alcun trattamento sui dati personali contenuti negli strumenti elettronici, fatta unicamente eccezione per i trattamenti di carattere temporaneo strettamente necessari per effettuare la gestione o manutenzione del sistema.

==========

Le lettere di incarico o di designazione degli incaricati vengono raccolte in modo ordinato e periodicamente, con cadenza almeno annuale, si procede ad aggiornare la definizione dei dati cui gli incaricati sono autorizzati ad accedere, e dei trattamenti che sono autorizzati a porre in essere, ciò al fine di verificare la sussistenza delle condizioni che giustificano tali autorizzazioni.
La stessa operazione viene compiuta per le autorizzazioni rilasciate ai soggetti incaricati della gestione o manutenzione degli strumenti elettronici.

==========

Sono previsti **interventi formativi degli incaricati del trattamento**, finalizzati a renderli edotti dei seguenti aspetti:
- profili della disciplina sulla protezione dei dati personali, che appaiono più rilevanti per l'attività svolta dagli incaricati, e delle conseguenti responsabilità che ne derivano
- rischi che incombono sui dati
- misure disponibili per prevenire eventi dannosi
- modalità per aggiornarsi sulle misure di sicurezza, adottate dal Titolare.

Tali interventi formativi sono programmati in modo tale da avere luogo al verificarsi di una delle seguenti circostanze:
- già al momento dell'ingresso in servizio
- in occasione di cambiamenti di mansioni, che implichino modifiche rilevanti rispetto al trattamento di dati personali
- in occasione della introduzione di nuovi significativi strumenti, che implichino modifiche rilevanti nel trattamento di dati personali.

Gli interventi formativi possono avvenire sia all'interno da parte di soggetti esperti nella materia, che all'esterno, presso soggetti specializzati.
Essi tendono a sensibilizzare gli incaricati sulle tematiche di sicurezza, facendo comprendere i rischi e le responsabilità (con specificazione delle connesse sanzioni penali e disciplinari) che riguardano il trattamento dei dati personali.

Gli interventi formativi pongono altresì come obiettivo la compiuta spiegazione del concetto di quale sia la natura ed il contenuto dei dati personali, sensibili e giudiziari, con l'invito a segnalare eventuali disfunzioni dei sistemi operativi.

In ogni caso, sono previste riunioni periodiche, almeno una volta l'anno, per fare il punto sull'evoluzione degli aspetti legati alla sicurezza nel trattamento dei dati personali.

3. Analisi dei rischi che incombono sui dati

E' stata compiuta l'analisi dei rischi che si può così sintetizzare.

Per i dati comuni del personale dipendente, dei candidati per l'instaurazione di un rapporto di lavoro, dei clienti-utenti, di terzi, dei fornitori, professionisti cui AMV spa affida incarichi, dagli stessi forniti o comunque acquisiti: il rischio legato alla loro gestione può definirsi medio/basso.

Per i dati sensibili e giudiziari del personale dipendente, dei clienti-utenti, di terzi, dagli stessi forniti o comunque acquisiti: il rischio legato alla loro gestione è da definirsi medio/basso, poiché il trattamento avviene esclusivamente all'interno dei locali di AMV spa.

Il rischio di accesso all'interno della sede aziendale da parte di soggetti non autorizzati può essere definito basso, atteso che l'ingresso nell'orario di apertura al pubblico è controllato da personale dipendente o da incaricati, e che i locali presentano le caratteristiche illustrate nel paragrafo 1.2.
Il rischio di accesso all'interno delle singole stanze - postazioni di lavoro di AMV spa - può essere definito medio in quanto pur risultando l'accesso di terzi alle postazioni di lavoro controllabile dal front office, il plesso è simultaneamente sede legale di altre società che operano con personale proprio.

Avendo adottato le disposizioni di sicurezza stabilite dal D.lgs. 81/2008 ed essendo presente il dispositivo "salvavita", il rischio elettrico e di incendi conseguenti può comunque definirsi basso.
Non può tuttavia escludersi che le aree ed i locali potrebbero essere interessati da eventi imprevedibili, quali incendi, allagamenti e corto circuiti, o possa verificarsi la possibilità che terzi malintenzionati accedano nei locali dove si svolge il trattamento (rapine, furti, danneggiamenti da atti vandalici).

Per quanto riguarda gli strumenti elettronici, il rischio di accesso ai dati in essi contenuti può essere definito basso, essendo state adottate le misure di sicurezza volte a ridurre il rischio di perdita e di accesso non autorizzato dei dati.
Non sono consentite duplicazioni di dati per finalità differenti da quelle stabilite per il trattamento.
Per quanto riguarda la documentazione cartacea, il rischio può essere definito basso, essendo gli archivi chiusi a chiave e gli armadi dotati di serrature ed essendo state adottate le altre misure indicate, fatta eccezione ovviamente per gli eventi imprevedibili.

Per quanto concerne i documenti ricevuti a mezzo fax il rischio di accesso non autorizzato alle informazioni in essi contenute è medio - basso, ciò in considerazione del posizionamento della macchina telefax posta in zona protetta da intrusioni di personale non autorizzato.

Per quanto riguarda i supporti di memorizzazione, il rischio di deterioramento dei dati in essi contenuti può essere ritenuto basso, attesi i frequenti back up, ed il fatto che essi sono conservati in armadi dotati di serrature, così come i supporti di installazione dei programmi software adottati, quando lasciati dai fornitori in disponibilità.

I PC presenti all'interno di AMV spa sono tra loro connessi in rete risultando ciascuno accessibile unicamente mediante digitazione di password personale, il loro impiego è possibile unicamente da parte dell'utilizzatore della singola postazione di lavoro.

Atteso – infine – che gli incaricati al trattamento dei dati sono qualificati ed affidabili e dimostrano riservatezza ed attenzione nella gestione dei dati stessi, il rischio legato ad atti di sabotaggio e ad errori umani, da parte del personale appartenente all'organizzazione di AMV spa o di persone che con esso hanno stretti contatti, può essere definito basso.
Per quanto riguarda i software contenuti negli strumenti elettronici, possono verificarsi errori e disfunzioni da virus, in relazione ai quali sono state applicate da parte dell'incaricato della gestione del sistema informativo opportune ed idonee contromisure, più avanti meglio specificate.

4. Misure atte a garantire l'integrità e la disponibilità dei dati

4.1 La protezione di aree e locali

I locali in cui sono conservati i dati personali trattati sono accessibili ai soggetti che vi svolgono stabilmente l'attività lavorativa, vale a dire tutti soggetti nominati Incaricati del trattamento dei dati personali.
Inoltre, accedono ai locali di AMV spa con frequenza stabilita nel contratto gli addetti dell'impresa di pulizia, del servizio postale e di consegna plichi.
L'eventuale accesso di terzi (clienti-utenti, fornitori, personale che svolge interventi di manutenzione di interni e di impianti elettrici, idraulici, informatici ecc.) avviene sempre durante l'orario di apertura di AMV spa e sotto il controllo diretto dei responsabili dei diversi uffici/ Incaricati del trattamento.
L'ingresso dei terzi in orari di apertura di AMV spa avviene normalmente secondo modalità ed orari concordati preventivamente, la porta d'ingresso non si apre con semplice spinta della stessa, ma esclusivamente dall'interno; i clienti-utenti vengono fatti accomodare nella zona d'attesa o subito ricevuti dall'ufficio front office o dagli uffici competenti, a seconda del motivo della visita.
La postazione ove è collocata l'ufficio front office consente di controllare i movimenti delle persone che passano dalla porta di ingresso e di quelle che si trovano in attesa di essere ricevute.
Le misure di sicurezza atte ad impedire l'accesso non autorizzato di estranei all'interno dei locali di AMV spa sono state già descritte nel paragrafo 1.2.
La porta interna in alluminio è tenuta sempre chiusa durante l'orario di apertura di AMV spa, e viene aperta unicamente previo azionamento di un comando interno una volta effettuato un riconoscimento visivo attraverso la vetrata di cui risulta in parte costituita la medesima porta.

La porta di accesso ad AMV spa è dotate di serrature di sicurezza, le cui chiavi sono possedute dal personale di AMV spa, dal personale dipendente di altre società e con le quali i rapporti sono regolamentati da contratti di servizio ed infine dagli addetti al servizio di pulizia.
Le porte di accesso delle stanze delle postazioni di lavoro, gli armadi, i cassetti in cui sono conservati i dati personali, sia quelli trattati su supporto cartaceo che quelli trattati su supporto informatico, sono dotati di serrature.
I PC, i supporti cartacei e supporti informatici sono conservati sollevati dal pavimento al fine di prevenire possibilità di distruzione o deterioramento in caso di allagamento.
La sede di AMV spa è dotata di più estintori regolarmente controllati, al fine di contrastare inizi di incendi.
Gli impianti ed i sistemi di cui è dotata la sede aziendale appaiono pertanto soddisfacenti al fine di garantire le opportune misure di sicurezza al trattamento di dati personali da esso svolti.

4.2 La custodia e l'archiviazione di atti, documenti e supporti

Per quanto concerne il reperimento, la custodia e l'archiviazione di atti, documenti e supporti diversi (ad esempio, CD, chiavette, …..), si è provveduto ad istruire gli incaricati, affinché adottino precise procedure atte a salvaguardare la riservatezza dei dati contenuti.

==========

Agli incaricati vengono date disposizioni, per iscritto, di accedere ai soli dati personali, la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati: in caso di dubbi, è stato loro prescritto di rivolgersi direttamente al proprio responsabile.
Di conseguenza, agli Incaricati è prescritto di prelevare dagli archivi i soli atti e documenti che vengono loro affidati per lo svolgimento delle mansioni lavorative, che devono controllare e custodire, durante l'intero ciclo necessario per lo svolgimento delle operazioni di trattamento, per poi restituirli all'archivio, al termine di tale ciclo.

==========

Gli Incaricati devono **custodire** in modo appropriato gli atti, i documenti ed i supporti contenenti dati personali, loro affidati per lo svolgimento delle mansioni lavorative.
Cautele particolari sono previste per gli atti, documenti e supporti contenenti dati sensibili e giudiziari: agli incaricati viene in questi casi prescritto di provvedere al controllo ed alla custodia in modo tale che ai dati non possano accedere persone prive di autorizzazione.
A tale fine, gli incaricati sono stati dotati di:

- cassetti con serratura
- armadi chiudibili a chiave

nei quali devono riporre i documenti, contenenti dati sensibili o giudiziari, prima di assentarsi dal posto di lavoro, anche temporaneamente. All'interno di tali dispositivi i documenti devono essere riposti anche al termine della giornata di lavoro, qualora l'incaricato debba continuare ad utilizzarli, nei giorni successivi. In caso di particolari esigenze lavorative o di ricerca è consentito lasciare temporaneamente atti e documenti sul tavolo di lavoro durante gli orari di chiusura di AMV spa, provvedendo tuttavia a garantire l'idonea chiusura della stanza al momento dell'allontanamento da essa da parte dell'incaricato.
Al termine del trattamento, l'incaricato dovrà restituire all'archivio gli atti, i documenti ed i supporti, non più necessari per lo svolgimento delle proprie mansioni lavorative.

==========

Per quanto concerne **l'archiviazione**, i Titolari hanno adibito apposite aree nelle quali conservare ordinatamente documenti, atti e supporti contenenti dati personali.

Nel rispetto dei principi di liceità, limitazione delle finalità e minimizzazione dei dati, ai sensi dell'art. 5 del GDPR, il periodo di conservazione dei dati personali è:

- stabilito per un arco di tempo non superiore al conseguimento delle finalità per le quali sono raccolti e trattati per l'esecuzione e l'espletamento delle finalità contrattuali;
- stabilito per un arco di tempo non superiore all'espletamento dei servizi erogati;
- stabilito per un arco di tempo non superiore al conseguimento delle finalità per le quali sono raccolti e trattati e nel rispetto dei tempi obbligatori prescritti dalla legge.

In qualunque momento, in conformità agli artt. 16 e 17 Reg., l'interessato potrà chiederne la cancellazione o la rettifica.

==========

Gli impianti e le attrezzature di cui sono dotati i diversi responsabile di settore, titolari per la custodia e l'archiviazione di atti, documenti e supporti, con particolare riferimento a quelli contenenti dati sensibili o giudiziari, oggetto di trattamento da parte di AMV spa appaiono soddisfacenti al fine di garantire la necessaria sicurezza ai dati personali contenuti in tali atti, documenti e supporti.

4.3 Le misure logiche di sicurezza

Per i trattamenti effettuati con **strumenti elettronici** (elaboratori, programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato), si adottano le seguenti misure:

4.3.1 - Il **sistema di autenticazione informatica** viene adottato per disciplinare gli accessi a tutti gli strumenti elettronici presenti all'interno di AMV spa.

Per realizzare le credenziali di autenticazione, si associa un codice per l'identificazione dell'incaricato (username), ad una parola chiave riservata (password), conosciuta solamente dall'incaricato, che provvederà ad elaborarla, mantenerla riservata e modificarla periodicamente.

Ad ogni incaricato esse vengono assegnate o associate individualmente, per cui non è ammesso che due o più incaricati possano accedere agli strumenti elettronici utilizzando la medesima credenziale.

Al verificarsi dei seguenti casi, è prevista la disattivazione delle credenziali di autenticazione:
- immediatamente, nel caso in cui l'incaricato perda la qualità, che gli consentiva di accedere allo strumento
- in ogni caso, entro sei mesi di mancato utilizzo, con l'unica eccezione delle credenziali che sono state preventivamente autorizzate per soli scopi di gestione tecnica, il cui utilizzo è quindi sporadico.

Le password sono composte da almeno otto caratteri.

Relativamente al sistema di autenticazione informatica sopra descritto, agli **incaricati vengono impartite precise istruzioni** in merito ai seguenti punti:
- obbligo di non lasciare incustodito e accessibile lo strumento elettronico, durante una sessione di trattamento, neppure in ipotesi di breve assenza
- dovere di elaborare in modo appropriato la password, e di conservare la segretezza sulla stessa, nonché sulle altre componenti riservate della credenziale di autenticazione (username), attribuite dall'amministratore di sistema. Agli incaricati è imposto l'obbligo di provvedere a modificare la password, con la seguente tempistica:
  - immediatamente, non appena viene consegnata loro da chi amministra il sistema
  - successivamente, almeno ogni sei mesi. Tale termine scende a tre mesi, se la password dà accesso ad aree in cui sono contenuti dati sensibili o giudiziari.

Le password sono composte da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non permetta una tale lunghezza, da un numero di caratteri pari al massimo consentito dallo strumento stesso.
Agli incaricati è prescritto di utilizzare alcuni accorgimenti nell'elaborazione delle password:
- esse non devono contenere riferimenti agevolmente riconducibili all'interessato (non solo nomi, cognomi, soprannomi, ma neppure date di nascita proprie…….), né consistere in nomi noti, anche di fantasia (pippo, pluto, paperino, …….)
- buona norma è che, dei caratteri che costituiscono la password, da un quarto alla metà siano di natura numerica.

La password non deve essere comunicata a nessuno (non solo a soggetti esterni). Nei casi di prolungata assenza o impedimento dell'incaricato, che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, potrebbe però rendersi necessario disporre della password dell'incaricato, per accedere agli strumenti ed ai dati. A tale fine, agli incaricati sono state fornite istruzioni scritte, affinché essi:

- scrivano la parola chiave su un foglio di carta, da inserire in una busta che deve essere chiusa e sigillata
- consegnino per la relativa custodia, la busta citata all'amministratore di sistema o a persona dallo stesso designata.

Solo al verificarsi delle condizioni, sopra esposte, che rendono necessario accedere allo strumento elettronico, l'amministratore di sistema potrà aprire la busta che il medesimo custodisce.
Dell'accesso effettuato si dovrà provvedere ad informare, tempestivamente, l'incaricato cui appartiene la parola chiave.

4.3.2. – Credenziali di autorizzazione
Si fa osservare che ogni dipendente ha un proprio ed autonomo profilo di autorizzazione nell'accesso al sistema informativo coerente alle mansioni e funzioni assegnate.

4.3.3 - Per quanto riguarda la **protezione di strumenti e dati** da malfunzionamenti, attacchi informatici e programmi che contengono codici maliziosi (virus), vengono adottate le misure sotto descritte.

Il primo aspetto (applicazione di **antivirus**, *marca mac Afee caratteristiche e configurazione di installazione*) riguarda la **protezione dei dati personali dal rischio di intrusione e dall'azione di programmi di cui all'articolo 615-quinquies del codice penale**, aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento (comunemente conosciuti come virus). A tale fine, si è dotati di idonei strumenti elettronici e programmi, che sono periodicamente aggiornati mediante ausilio di specifico software.

Tutti gli incaricati sono stati istruiti, in merito all'utilizzo dei programmi antivirus e, più in generale, sulle norme di comportamento da tenere, per minimizzare il rischio di essere contagiati: a tale fine, è stato loro distribuito un codice dei comportamenti da tenere, e di quelli da evitare.

Il secondo aspetto (applicazione di **firewall**, *marca Watchguard, caratteristiche e configurazione di installazione*) riguarda la **protezione degli elaboratori dall'accesso abusivo, di cui all'articolo 615-ter del codice penale**, ai sensi del quale compie tale reato chi si introduce abusivamente in un sistema informatico o telematico, protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.
La protezione da tali accessi avviene mediante l'impiego di idonei strumenti elettronici, comunemente conosciuti come firewall, obbligatori nei casi in cui si trattino dati sensibili o giudiziari.

A tale riguardo la nostra organizzazione si è da tempo dotata di tali strumenti, per la protezione dei diversi PC.

4.3.4. - Per quanto concerne i **supporti rimovibili** (es. chiavette, CD, DVD….), contenenti dati personali, la norma impone particolari cautele solo nell'ipotesi in cui essi contengano dati sensibili o giudiziari.

La nostra organizzazione ha ritenuto di estendere tali precetti ai supporti contenenti dati personali di qualsiasi natura, anche comune, prescrivendo agli incaricati del trattamento quanto segue:

- i supporti devono essere custoditi ed utilizzati in modo tale da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti: in particolare, essi devono essere conservati in cassetti chiusi a chiave, durante il loro utilizzo, e successivamente formattati, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi
- una volta cessate le ragioni per la conservazione dei dati, si devono in ogni caso porre in essere gli opportuni accorgimenti, finalizzati a rendere inintelligibili e non ricostruibili tecnicamente i dati contenuti nei supporti. Tali dati devono quindi essere cancellati, se possibile, e si deve arrivare addirittura a distruggere il supporto, se necessario per i fini in esame.

Le misure logiche di sicurezza, di cui è dotato il Titolare per la protezione dei trattamenti che avvengono con strumenti elettronici appaiono nel loro complesso soddisfacenti, al fine di garantire la necessaria sicurezza ai dati personali trattati.

5. Criteri e modalità di ripristino dei dati

Per fronteggiare le ipotesi in cui i dati siano colpiti da eventi che possano danneggiarli, o addirittura distruggerli, vengono previsti criteri e modalità tali da garantire il loro ripristino in termini ragionevoli, e comunque entro una settimana per i dati sensibili e giudiziari. Per i dati trattati con strumenti elettronici, sono previste procedure di **backup**, attraverso le quali viene periodicamente effettuata una copia di tutti i dati presenti nel sistema, su dispositivi opportuni (CD, backup online…..).
Il salvataggio dei dati trattati avviene come segue:

- la frequenza dell'operazione è settimanale;
- si utilizzano supporti differenti da quelli in cui sono contenuti i dati dei salvataggi eseguiti la volta precedente;
- per ciascun salvataggio, si esegue 1 copia.

Le copie vengono custodite presso il locale CED.

Nell'ipotesi di distruzione o danneggiamento dei dati o degli strumenti elettronici, l'amministratore di sistema nominato deve:

- avvertire il Titolare del trattamento dei dati e recuperare i supporti di back up nonché quelli contenenti i vari software di AMV spa installati sugli strumenti elettronici;
- rivolgersi immediatamente e chiedere l'intervento della società incaricata, sollecitandone al più presto l'assistenza;
- con l'ausilio del consulente informatico, reinstallati i programmi danneggiati o distrutti, sempre che non sia necessario sostituire l'intero hardware, provvedere a reinstallare tutti i dati contenuti nei supporti di back up;
- con l'ausilio del consulente informatico, provvedere all'aggiornamento dei sistemi operativi una volta reinstallati;
- in ogni caso, viene data esplicita istruzione che il ripristino dei dati e dei sistemi sia effettuato entro e non oltre 7 giorni;

Al fine di evitare la perdita ed il danneggiamento degli strumenti elettronici e dei dati in essi contenuti, è effettuata l'ordinaria manutenzione dei sistemi elettronici dall'amministratore del Sistema con il supporto del/i tecnico/i incaricato/i. Ai sensi dell'art. 33 GDPR, nel caso in cui vi sia una violazione dei dati personali, il Titolare del trattamento, senza indugi – e in ogni caso entro 72 ore - notificherà la violazione all'autorità di controllo competente a norma dell'art. 55.

6. L'affidamento di dati personali all'esterno

Nei casi in cui i trattamenti di dati personali vengano affidati all'esterno della struttura di AMV spa, si adottano i seguenti criteri, atti a garantire che il soggetto destinatario adotti misure di sicurezza conformi a quelle minime. Per la generalità dei casi in cui il trattamento di dati personali, **di qualsiasi natura**, venga affidato all'esterno dell'azienda, sono impartite istruzioni per iscritto al terzo destinatario, di rispettare quanto prescritto per il trattamento dei dati personali.
Ai sensi dell'art. 45 GDPR il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche. Qualora il trasferimento avvenga verso soggetti non considerati sicuri per il trattamento dei dati personali, si stipulano con il destinatario clausole contrattuali conformi ovvero si forniscono, in ogni caso, garanzie adeguate. Nei casi in cui ciò si renda opportuno, per ragioni operative legate anche alla tutela dei dati personali, il destinatario esterno viene nominato dal Titolare come responsabile/incaricato del trattamento dei dati, mediante apposita comunicazione.

7. Controllo generale sullo stato della sicurezza

Al Titolare è affidato il compito di aggiornare le misure di sicurezza, al fine di adottare gli strumenti e le conoscenze, resi disponibili dal progresso tecnico, che consentano di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito.

Al fine di verificare l'efficacia delle misure di sicurezza adottate, il Titolare, con l'ausilio del consulente informatico, provvedono con frequenza semestrale, anche tramite controlli a campione, ad effettuare una o più delle seguenti attività:

- verificare l'accesso fisico ai locali dove si svolge il trattamento
- verificare la correttezza delle procedure di archiviazione e custodia di atti, documenti e supporti contenenti dati personali
- monitorare l'efficacia ed il corretto utilizzo delle misure di sicurezza adottate per gli strumenti elettronici
- verificare l'integrità dei dati e delle loro copie di backup
- verificare la sicurezza delle trasmissioni in rete
- verificare che i supporti magnetici, che non possono più essere riutilizzati, vengano distrutti
- verificare il livello di formazione degli incaricati.

Almeno ogni sei mesi, si procede ad una sistematica verifica del corretto utilizzo delle parole chiave e dei profili di autorizzazione che consentono l'accesso agli strumenti elettronici da parte degli incaricati, anche al fine di disabilitare quelli che non sono stati mai utilizzati nell'arco del semestre di riferimento.

8. Considerazioni conclusive e conseguenze applicative

Il presente documento scaturisce dall'analisi delle necessità conseguenti all'entrata in vigore del Regolamento UE 679/2016 citato in premessa.
In esecuzione di ciò si è provveduto con atto separato (che costituisce parte integrante del presente documento e per tale motivo anche a questo allegato), redatto a cura del legale rappresentante, Titolare del Trattamento , all'individuazione e nomina dei soggetti incaricati del trattamento dei dati personali ed alla specificazione scritta ed analitica dei compiti loro affidati ed i termini dell'autorizzazione al trattamento dei dati comuni, sensibili e giudiziari che non siano già contemplati dal presente documento.
Ai destinatari delle comunicazioni precedenti è allegata anche copia datata e firmata in originale del presente documento, perché funga da istruzione circa i compiti e le norme da osservare nell'ambito dell'attività svolta presso AMV spa.
Il presente documento viene sottoscritto dal Titolare e conservato in originale presso AMV spa viene diffuso nella rete aziendale in idonea cartella, unitamente all'atto di nomina con relative istruzioni firmate per accettazione dai destinatari.
Ad esso saranno uniti i documenti che in futuro costituiranno integrazione ed aggiornamento del presente atto, necessari per adeguarsi a successive disposizioni di leggi o regolamenti, ovvero a diversa organizzazione di AMV spa per la parte che attiene all'organigramma, ai locali ed agli strumenti informatici o comunque automatizzati.

9. Dichiarazioni d'impegno e firma

Il presente documento, redatto in data odierna viene firmato in calce dall'amministratore unico della società, legale pro tempore in qualità di Titolare del trattamento.

L'originale del presente documento viene custodito presso la sede aziendale per essere esibito in caso di controlli e messo a disposizione della rete aziendale in idonea cartella.
Una sua copia verrà consegnata:

- ai responsabili/incaricati esterni del trattamento dei dati personali
- a chiunque ne faccia richiesta, in relazione all'instaurarsi di un rapporto che implichi un trattamento congiunto di dati personali.

Il presente documento potrà subire aggiornamenti a seguito di adeguamenti normativi ed organizzativi che saranno opportunamente divulgate.

Valenza, 25 maggio 2018

L'amministratore unico di AMV spa
(geom. Marcello Omodeo)
f.to in originale