DOCUMENTO DI IMPATTO SULLA PROTEZIONE DEI DATI EX ART. 35 G.D.P.R.

PREMESSA

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 dell'Azienda Elettrogruppo ZeroUno S.p.a., sede legale Strada San Mauro, 191, cap 10156 Torino, c.f./p.iva 00526610019 rappresentata dal Sig. Giovanni Paolo Terzolo, nato a Nizza Monferrato (AT) il 29/04/1960, c.f. TRZGNN60D29F902N, nell'ambito della sua attività di Amministratore Delegato.

Indice

1. Elenco dei trattamenti dei dati personali

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

Ufficio

Il trattamento dei dati personali avviene all'interno dell'Azienda, presso le unità locali di riferimento, debitamente elencate nell'All. 1

L'accesso agli uffici di ogni unità locale è regolato da opportuni sistemi di controllo e di sicurezza.

Tali sistemi di controllo e sicurezza sono elencati per ogni unità locale nell'All. 2

I locali destinati all'archivio cartaceo sono individuati per ogni unità locale e risultano chiusi con idonea serratura a chiavi, le cui copie sono in possesso dei Preposti di ogni unità locale e custodite in una cassetta di sicurezza.

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, per ordine alfabetico e suddivisi per categorie, per essere archiviati all'interno di armadi ciascuno dotato di chiusura a chiave.

B – Elaboratori eroganti servizi all'interno dell'azienda

Si intendono quelli accessibili ai soli elaboratori facenti parte della rete dati interna all'azienda ("intranet"), attraverso connessioni fisicamente o virtualmente private, cioè attraverso la connessione fisica della rete locale oppure attraverso un canale di trasmissione cifrato (rete privata virtuale). Essi sono dislocati presso il Centro Elaborazione Dati di Beinasco (TO), via Aosta 15. L'accesso ai loro servizi è protetto da apposite credenziali personali, mentre l'accesso dall'esterno per il tramite della rete privata virtuale è ammesso da apposita apparecchiatura "firewall", che garantisce anche l'irraggiungibilità di tali server da reti o apparati non autorizzati. Essi sono:

- due server che erogano i servizi del sistema informativo aziendale ERP "Elettrix" e della relativa base dati (Applicaton server e Database server)
- due server che erogano i servizi di portale intranet aziendale e della relativa banca dati (Applicaton server e Database server)
- un server che eroga i servizi di consultazione dei dati di Business Intelligence
- un server incaricato delle procedure di riapprovvigionamento di magazzino ed ottimizzazione delle scorte
- un server incaricato dell'archiviazione sostitutiva e gestione documentale con l'uso del software applicativo "Arxivar"
- due server incaricati di condividere cartelle, uno ad uso degli uffici amministrativi ed uno ad uso degli uffici direzionali.

E' altresì presente presso la Server Farm della società Elmec di Brunello (VA) un server incaricato del test delle nuove procedure di riapprovvigionamento di magazzino ed ottimizzazione delle scorte. L'accesso a tale server è protetto da apposita apparecchiatura "firewall" ed è ammesso soltanto attraverso rete privata virtuale stabilita tra il CED di Beinasco (TO) e la Server Farm della società Elmec di Brunello (VA), nonché da apposite credenziali in possesso delle sole persone autorizzate ad accedervi. La società Elmec ha predisposto quanto necessario a rispondere ai requisiti di tutela e protezione dei dati personali presenti su tale server, in piena rispondenza alle normative vigenti.

C – Elaboratori eroganti servizi raggiungibili da rete pubblica

Si intendono quelli accessibili a qualsiasi elaboratore collegato alla rete Internet. L'accesso è ammesso attraverso un indirizzo IP pubblico per ogni server; ad esso corrisponde una stringa univoca, di facile memorizzazione, utilizzabile nei programmi di navigazione. Parte di essi è dislocata presso il Centro Elaborazione Dati di Beinasco (TO), via Aosta 15, un'altra parte presso la sala server scelta dal fornitore pro tempore del servizio. In entrambi i casi l'accesso ai dati personali è protetto da userid e password ed i servizi sono erogati attraverso il filtro di apposite apparecchiature "firewall" che rendono pubblicamente disponibili i soli canali attraverso i quali sono erogati i servizi (in termine tecnico, "porte"). Essi sono:

- un server che eroga il servizio del sito istituzionale aziendale, affidato alla società Emoe
- un server che eroga il servizio di consultazione articoli, prezzi, disponibilità e permette di inserire ordini dalla rete internet, convenzionalmente denominato "Web Order" , presente presso il Centro Elaborazione Dati di Beinasco (TO)
- un server che eroga il servizio di Customer Relationship Management, presente presso il Centro Elaborazione Dati di Beinasco (TO).

Sono paragonabili a questi server, per la tipologia di accesso e il tipo di dati presenti, le apparecchiature di videosorveglianza e registrazione dislocate presso i vari punti vendita.

L'accesso ad esse è disponibile con modalità analoghe a quelle sopra indicate: indirizzo IP pubblico, "porte" accessibili limitate dall'apparecchiatura firewall, accesso tramite apposite credenziali. Esse sono dislocate presso:

- il magazzino centrale di Beinasco (TO), via Aosta 15
- il magazzino cavi di Beinasco (TO), strada San Luigi 1
- il punto vendita clima di Beinasco (TO), strada San Luigi 1
- il punto vendita materiale elettrico e termoidraulica di Beinasco (TO), via Aosta 3

- il punto vendita di Alessandria, via Rosa Piacentini Rivera 7
- il punto vendita di Asti, via Learco Guerra 24
- il punto vendita di Carmagnola (TO), via dell'Industria "90" 23
- il punto vendita di Casale Monferrato (AL), via Achille Grandi 24
- il punto vendita di Cuneo, frazione Madonna dell'Olmo, via Molino Roero 3/C
- il punto vendita di Moncalieri (TO), strada Genova 216/A
- il punto vendita di Rivarolo (TO), corso Re Arduino 69
- il punto vendita di Venaria Reale (TO), strada Druento 254.

Per ragioni specifiche di marketing, Elettrogruppo Zerouno Spa può affidarsi ad ulteriori fornitori, quale ad esempio il consorzio FINDEA per la gestione del programma promozionale MAXILIFE, per rendere accessibili alcune opportunità commerciali. In tutti i casi Elettrogruppo Zerouno Spa esige dal fornitore, anche pro-tempore, il rispetto dei requisiti di sicurezza d'accesso elencati all'inizio del presente capoverso.

D – Elaboratori fissi senza accesso alla rete pubblica

Si intendono quelli che accedono soltanto ai servizi erogati dai server presenti nella rete interna. Sono dislocati presso i diversi punti vendita secondo lo schema più sotto riportato e corrispondono a due distinti modelli:

- uno stabilmente collocato presso una postazione e definito "thin client"
- uno mobile, dotato di lettore per i codici a barre, destinato soltanto alla movimentazione di magazzino, che utilizza software apposito, definito "terminale in radiofrequenza".

E – Elaboratori fissi e mobili aventi accesso alla rete pubblica

Si intendono quelli che accedono ai servizi erogati dai server presenti nella rete interna ed a quelli presenti in Internet. Sono dislocati presso i diversi punti vendita secondo lo schema più sotto riportato e convenzionalmente definiti "personal computer (abbreviato p.c.) fissi" quando stabilmente collocati presso la singola postazione, "p.c. mobili" quando integrano processore e monitor in un'unica entità hardware facilmente trasportabile e sono altresì commercialmente definiti, a seconda dello specifico allestimento hardware, "laptop", "tablet", "convertibili" o "portatili".

Gli elaboratori mobili possono accedere ai servizi della rete interna anche quando si trovano al di fuori della rete aziendale in maniera sicura e protettiva del dato consultato, stabilendo una rete privata virtuale, con le modalità più sopra descritte in merito ai server elencati al punto B).

Tutti questi elaboratori sono configurati in modo da scaricare ed installare automaticamente tutti gli aggiornamenti software previsti dal produttore del sistema operativo su di essi installato e riconducibile ai due produttori mondiali Microsoft ed Apple. Tutti gli elaboratori dotati di sistema operativo Microsoft sono altresì dotati di programma antivirus aggiuntivo parimenti aggiornato.

L'accesso ai servizi Internet è regolamentato da apposite policy sulle apparecchiature firewall, che vietano l'accesso a siti appartenenti a categorie non inerenti l'attività lavorativa.

Schema riportante il parco hardware installato

Sede	Rif. E) N. p.c. fissi	Rif. E) N. p.c. portatili	D) N. thin client	D) N. terminali r.f.
Uffici direzionali, Beinasco (TO), via Aosta 15	22	10	0	0
Magazzino centrale, Beinasco (TO), via Aosta 15	11	0	5	42
Magazzino cavi, Beinasco (TO), strada San Luigi 1	2	0	0	5
Punto vendita clima, Beinasco (TO), strada San Luigi 1	6	0	0	3
Punto vendita materiale elettrico e termoidraulica, Beinasco (TO), via Aosta 3	18	12	0	20
Uffici amministrativi, Beinasco (TO), via Aosta 3	17	1	0	0
Punto vendita Burolo (TO), via Mombarone 5	7	1	0	0
Punto vendita Ciriè (TO), via Remmert 77	7	2	2	3
Punto vendita Asti, via Learco Guerra 24	7	3	0	2

Punto vendita Canelli (AT), strada dell'Antica Fornace 14	5	0	1	3
Punto vendita Borgomanero (NO), via Novara 380	9	4	0	4
Punto vendita Novara, corso Trieste 108	7	3	0	2
Punto vendita Domodossola, strada statale del Sempione – Regione Nosere 6	5	0	0	0
Punto vendita Feriolo di Baveno (VB), strada statale del Sempione 72	4	1	0	0
Punto vendita Cuneo fraz. Madonna dell'Olmo, via Molino Roero 3/C	9	5	0	2
Punto vendita Guarene (CN), via Carmagnola 6/A	7	3	1	2
Punto vendita Avigliana (To), corso Torino 8/B	5	0	0	2
Punto vendita Alessandria, via Rosa Piacentini Rivera 7	7	1	1	3
Punto vendita Venaria Reale (TO), strada Druento 254	15	6	2	4
Punto vendita Casale Monferrato (AL), via Achille Grandi 24	4	2	0	3
Punto vendita Acqui Terme (AL), via Alberto da Giussano 56	8	2	0	0
Punto vendita Moncalieri (TO), strada Genova 216/A	5	1	0	0
Punto vendita Torino, strada San Mauro 151	15	5	1	4
Punto vendita Rivoli, viale Nuvoli 8/B	2	0	0	0
Punto vendita Genova, via Giuseppe Bertuccioni 34 b rosso	16	3	0	2
Punto vendita Rivarolo Canavese (TO), corso Re Arduino 69	6	1	0	2
Punto vendita Mondovì, via Viadotto 24	4	0	0	0
01 Concept Store, punto consulenza e vendita illuminotecnica, Torino, corso Tortona 60	6	3	0	0
Punto vendita Carmagnola, via dell'Industria "90" 23	9	1	0	0

2. Interventi formativi degli incaricati

Incaricati del trattamento:
hanno accesso ai dati personali:

- tutti i dipendenti di Elettrogruppo ZeroUno S.p.a.;
- i professionisti legati a Elettrogruppo ZeroUno S.p.a. da un contratto di Agenzia

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 l'inserimento dei dati,
- modalità di reperimento dei documenti, contenenti dati personali, e modalità da osservare per la custodia dei supporti cartacei e la loro archiviazione, al termine dello svolgimento del lavoro
- obbligo di segretezza della password che viene rilasciata dal Centro Elaborazione Dati interno ad Elettrogruppo ZeroUno S.p.a. con modalità ad personam, necessaria per accedere agli elaboratori elettronici ed ai dati in essi contenuti
- prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici

Tutti gli incaricati del trattamento sono tenuti a sottoscrivere un obbligo di riservatezza con il quale si impegnano a non divulgare in alcun modo a terzi i dati personali, anche sensibili, di cui siano venuti a conoscenza alla luce del loro legittimo specifico incarico (se non per le specifiche finalità e con le modalità contenute nella presente informativa sul trattamento dei dati personali).

Società fornitrici incaricate dell'assistenza e manutenzione degli strumenti elettronici sono:

- VM Sistemi S.p.A. con sede in Faenza (RA), via R. Ossani 18, per quanto inerente la piattaforma hardware, il sistema operativo, il database ed il software applicativo ERP "Elettrix"; il sistema operativo, il database ed il software applicativo di acquisto online "Web Order"; il software di archiviazione sostitutiva e gestione documentale "Arxivar" con relativo database;
- 3C Informatica s.r.l. con sede in Savigliano, corso Isoardi 60, per quanto inerente la piattaforma hardware, il sistema operativo ed il database dei server che garantiscono i servizi di portale intranet;
- Tour Data Program di G. Setzu & C., con sede in VIA Santa Maria Mazzarello 94, Torino, per quanto inerente la piattaforma hardware, il sistema operativo, il database ed il software di gestione della "Customer Relationship Management";
- SETI s.r.l. con sede in Torino, Via C. Pittara 14, per quanto inerente la piattaforma hardware di tutti i rimanenti server, l'installazione e manutenzione hardware e software di parte delle postazioni p.c.;
- Bellucci s.r.l. con sede in Torino, via Fratelli Savio 2, per quanto inerente l'installazione e manutenzione hardware e software della rimanente parte di postazioni p.c.
- Kelyan S.p.A. con socio unico, con sede in Torino, via XX Settembre 17, per quanto inerente l'installazione e manutenzione hardware e software degli apparati "firewall".

Gli interventi che non hanno impatto sul trattamento di dato alcuno (es. manutenzione ai terminali in radiofrequenza) possono essere svolti dal personale di altre società non elencate.
Alle società fornitrici sopra elencate 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.
Il rispetto delle norme previste dal regolamento è garantito dalla sorveglianza che il personale dipendente di Elettrogruppo ZeroUno S.p.a. svolge sull'operato del personale di dette società.

Inoltre, alle stesse vengono impartite istruzioni circa:
- 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 degli eventuali supporti rimuovibili, contenenti dati personali
- dovere di aggiornarsi, utilizzando il materiale e gli strumenti forniti dal Titolare, sulle misure di sicurezza.

==========

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:
- 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, a cura dei Titolari o di altri 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 sensibili e giudiziari, con l'invito a segnalare eventuali disfunzioni dei sistemi operativi e, nel dubbio, di richiedere ai Titolari se un dato possa avere o meno natura sensibile o giudiziaria.
In ogni caso, sono previste riunioni periodiche, in numero di 1 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 clienti, di terzi, dei fornitori, degli altri professionisti con cui l'Azienda intrattiene legami di natura commerciale, dagli stessi forniti o comunque acquisiti: il rischio legato alla loro gestione può definirsi basso.

Il rischio di accesso all'interno delle Unità Locali dell'Azienda da parte di soggetti non autorizzati può essere definito basso, atteso che l'ingresso nell'orario di apertura è controllato da personale dipendente o da incaricati, e che i locali presentano le caratteristiche illustrate nell'All. 2.
Il rischio di accesso all'interno delle singole stanze delle Unità Locali può essere definito basso, atteso che l'ingresso di terzi estranei avviene solo previa accettazione e controllo.
Il rischio di accesso alle singole postazioni di lavoro da parte di persone non autorizzate può essere definito basso, poiché è controllato l'accesso di terzi all'interno dei locali delle Unità Locali e l'eventuale tempo di attesa è monitorato dal personale
Avendo adottato le disposizioni di sicurezza stabilite dal D.lgs. 81/2008 ed essendo presenti il dispositivo "salvavita", e gli estintori previsti per ogni singola unità locale, 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 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 basso, ciò in considerazione del posizionamento delle macchine telefax poste 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 ignifughi e dotati di serrature , così come i supporti di installazione dei programmi software adottati, quando lasciati dai fornitori in disponibilità.

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 dell'Azienda o di persone che con essa 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.

Si dà atto che l'Azienda utilizza processi automatizzati, al sol fine di stabilire un blocco degli acquisti per coloro che raggiungono la capienza del limite di fido concesso.

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.
L'eventuale accesso di terzi (clienti, fornitori, personale che svolge interventi di manutenzione di interni e di impianti elettrici, idraulici, informatici ecc.) avviene sempre durante l'orario di apertura dell'Azienda e sotto il controllo diretto dei Titolari o di uno degli incaricati.
L'ingresso dei terzi in orari di apertura dell'Azienda avviene normalmente secondo modalità ed orari concordati preventivamente, le porte d'ingresso non si aprono con semplice spinta delle stesse, ma esclusivamente dall'interno tramite comando elettrico attivato dal personale; i clienti vengono accompagnati dal dipendente con cui hanno appuntamento.
Le misure di sicurezza atte ad impedire l'accesso non autorizzato di estranei all'interno dei locali dell'Azienda sono state già descritte nel paragrafo 1.1.
Elaboratori, supporti cartacei e supporti informatici sono conservati sollevati dal pavimento al fine di prevenire possibilità di distruzione o deterioramento in caso di allagamento.
L'azienda è dotata di più estintori regolarmente controllati, al fine di contrastare inizi di incendi.

Gli impianti ed i sistemi di cui è dotato l'Azienda appaiono pertanto soddisfacenti al fine di garantire le opportune misure di sicurezza al trattamento di dati personali da esso svolti.
Per l'anno 2018 sono quindi previsti semplici interventi di manutenzione.

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

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

==========

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

L'archivio DEI DOCUMENTI è collocato all'interno di più locali, e la sicurezza dei dati in esse contenuti è garantita mediante l'adozione dei seguenti accorgimenti:

- l'accesso all'archivio è consentito unicamente ai soggetti incaricati al trattamento ai quali viene consegnata la chiave di apertura del locale - locale adibito esclusivamente a tale scopo;
- La chiave di accesso all'archivio è in possesso del Preposto designato per ogni unità locale.

- Il Preposto ha il compito di procedere mensilmente ad almeno n. 1 controllo da espletarsi all'interno del locale adibito ad archivio, al fine di verificare la regolare conservazione ed integrità del materiale ivi contenuto;

Dopo l'orario di chiusura dell'Azienda, l'accesso all'archivio è consentito unicamente ai Titolari.
Si dà atto che i dati non più utilizzati verranno eliminati entro il termine di DIECI anni. 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 Titolari per la custodia e l'archiviazione di atti, documenti e supporti, oggetto di trattamento da parte dell'Azienda, appaiono soddisfacenti al fine di garantire la necessaria sicurezza ai dati personali contenuti in tali atti, documenti e supporti.
Per l'anno 2018 sono quindi previsti semplici interventi di manutenzione.

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 dell'Azienda.

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 e dal responsabile dei sistemi informativi pro-tempore.
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.
Ogni incaricato è stato adeguatamente formato all'elaborazione e modifica della password.
E' prevista la disattivazione delle credenziali di autenticazione nel caso in cui l'incaricato perda la qualità, che gli consentiva di accedere allo strumento
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 conservare la segretezza sulla password assegnata, nonché sulle altre componenti riservate della credenziale di autenticazione

La password non deve essere comunicata a nessuno (non solo a soggetti esterni, ma neppure a persone appartenenti all'Azienda, siano esse colleghi, dirigenti o titolare).

4.3.2 - 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 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 programma antivirus Sophos, aggiornato tutte le volte che il terminale entra in rete e più volte al giorno.

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, viene periodicamente inviata a tutti gli incaricati una mail contenente le opportune raccomandazioni in merito a comportamenti da tenere e da evitare assolutamente.

Il secondo aspetto (applicazione di **firewall**), 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 l'Azienda si è da tempo dotata di tali strumenti, per la protezione degli elaboratori presenti nel centro elaborazione dati di Beinasco ed elencati ai precedenti punti 1..B e 1.C, di apparecchiatura firewall prodotta dalla società CheckPoint, fornita e regolarmente manutenuta dalla società Kelyan, di cui al precedente punto 2 terzo capoverso.
I punti vendita dotati di apparecchiatura di videosorveglianza la rendono disponibile alla rete pubblica soltanto attraverso apposita apparecchiatura firewall.
In entrambi i casi i firewall consentono l'accesso ai server ovvero alle apparecchiature di videosorveglianza raggiungibili dalla rete pubblica ammettendo l'accesso attraverso un numero limitato di "porte". Il singolo server ammette poi l'accesso soltanto attraverso apposite credenziali.

4.3.3. - 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.

L'azienda 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.
Per l'anno 2018, sono quindi previsti semplicemente interventi finalizzati all'aggiornamento e alla manutenzione.

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,.
Doverosamente si premette che tutti i dati presenti nei diversi server elencati ai precedenti punti 1..B e 1..C sono replicati in tempo reale su supporti fisici (dischi fissi ovvero "hard disk") diversi all'interno dello stesso server, utilizzando la tecnica del "mirroring", in modo tale che l'impatto di un guasto hardware che interessi un disco fisso non causi distruzione o perdita dei dati, purchè si provveda rapidamente alla

sostituzione della parte guasta. A tal fine i server interessati sono sottoposti, qualora fuori dal periodo di garanzia, a regolare contratto di manutenzione con tempi certi di ripristino della parte guasta.

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 giornaliera;
- si utilizzano supporti differenti da quelli in cui sono contenuti i dati dei salvataggi eseguiti la volta precedente, mantenendo quattro copie precedenti (il lunedì si sovrascrive la copia effettuata il lunedì precedente);
- per ciascun salvataggio, si esegue 1 copia;
- Le copie sono custodite in armadio ignifugo in locale diverso dalla sala dove sono installati i server, sui quali sono memorizzati i dati.

Per i dati trattati con strumenti elettronici nei sistemi accessori descritti ai precedenti punti 1.B e 1.C, viene giornalmente effettuata copia integrale dei server virtualizzati attraverso la tecnica del "backup incrementale" (soltanto le differenze rispetto al precedente backup) mentre una copia integrale ("backup completo") viene effettuata settimanalmente.
Sia il backup completo, sia il backup incrementale risiedono su uno dei server che offrono il servizio di cartelle condivise, all'interno della stessa sala dove sono installate i server, ma su diverso supporto fisico.

Le copie di riserva dei dati presenti sui server non dislocati presso il Centro Elaborazione Dati di Beinasco e le modalità del loro ripristino sono demandate al fornitore pro tempore del servizio, dettagliato ai precedenti punti 1.B e 1.C, e sono oggetto di specifico contratto di fornitura che prevede modalità identiche a quelle descritte nel precedente paragrafo.

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

- avvertire il Titolare del trattamento dei dati e recuperare i supporti di back up nonché quelli contenenti i vari software dell'Azienda installati sugli strumenti elettronici;
- rivolgersi immediatamente e chiedere l'intervento del/dei tecnico/tecnici manutentore dell'Azienda, indicati al precedente punto 2., per la parte di competenza, 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;
- verrà dato incarico al tecnico manutentore di suggerire ogni altra misura;
- 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 dal tecnico incaricato.

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. Controllo generale sullo stato della sicurezza

Ai Titolari 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, i Titolari, 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; a tal fine è stato implementato un sistema di notifica a mezzo e-mail dei back-up non andati a buon fine
- verificare che i supporti magnetici, che non possono più essere riutilizzati, vengano distrutti
- verificare il livello di formazione degli incaricati.

7. Considerazioni conclusive e conseguenze applicative

Il presente documento scaturisce dall'analisi dei problemi conseguenti all'entrata in vigore del Regolamento UE 679/2016 citato in premessa.
Il presente documento viene sottoscritto dai Titolari e conservato in originale presso l'Azienda, unitamente alle nomine con istruzioni firmate per accettazione dai destinatari.
Viene altresì pubblicato sul sito www.egzerouno.com
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 dell'Azienda per la parte che attiene all'organigramma, ai locali ed agli strumenti informatici o comunque automatizzati.

8. Dichiarazioni d'impegno e firma

Il presente documento, redatto nell'Aosto 2019, viene firmato in calce da:

- Elettrogruppo ZeroUno S.p.a., Sig. Giovanni Paolo Terzolo.

L'originale del presente documento viene custodito presso l'Azienda, per essere esibito in caso di controlli.
Una sua copia verrà consegnata:

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

Torino, lì 03-08-2019

Il Titolare. ELETTROGRUPPO ZEROUNO S.p.A.