UNINDUSTRIA SERVIZI

# REGOLAMENTO PER LA PROTEZIONE DEI DATI

*** *** ***

***REDATTO AI SENSI E PER GLI EFFETTI DELL'ARTICOLO 34, COMMA 1, LETTERA G) DEL D.LGS 196/2003 e successive modifiche, e del disciplinare tecnico allegato al medesimo decreto sub b)***
***e dell'art. 24 del GDPR n. 679/2016***

# REGOLAMENTO PER LA PROTEZIONE DEI DATI

Scopo del presente Documento ("RPD") è quello di delineare il quadro delle misure di sicurezza, organizzative, fisiche e informatiche, adottate e da adottarsi per il trattamento dei dati personali effettuato da Unindustria Servizi S.r.l., con sede legale in Como (CO), Via Raimondi n. 1, (il "Titolare") in persona del Presidente C.d.A. Antonella Mazzoccato, quale legale rappresentante *pro tempore*.

==========

Conformemente al disposto del Disciplinare Tecnico, allegato al D.Lgs. 196/2003, punto 19, ed al GDPR n. 679/2016 nel presente documento sono fornite idonee informazioni riguardanti:

1. l'elenco dei trattamenti di dati personali;
2. la distribuzione dei compiti e delle responsabilità, nell'ambito delle strutture preposte al trattamento dei dati e previsione di interventi formativi rivolti agli incaricati del trattamento;
3. l'analisi dei rischi che incombono sui dati;
4. le misure necessarie per garantire l'integrità e la disponibilità dei dati nonché la protezione di aree e locali rilevanti ai fini della relativa custodia ed accessibilità;
5. i criteri e le modalità di ripristino dei dati in seguito a distruzione o danneggiamento;
6. i criteri da adottare, per garantire l'adozione delle misure minime di sicurezza, in caso di trattamenti di dati personali affidati all'esterno con particolare riferimento al trasferimento dei dati extra UE.

**INDICE**

## CAPITOLO 1 - ELENCO DEI TRATTAMENTI DEI DATI PERSONALI

L'elenco in merito ai trattamenti dei dati personali posti in essere dal Titolare è rappresentato dalla mappatura di tali dati e dalla descrizione delle aree, locali e strumenti con i quali e presso i quali si effettuano detti trattamenti.

### 1.1 Mappatura dei dati trattati

La mappatura dei dati trattati dal Titolare, con l'indicazione della tipologia dei dati, della eventuale sensibilità degli stessi, del tipo di trattamento, vengono sintetizzati nel registro di trattamento dei dati che costituisce parte integrante del presente documento (allegato 1).

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

Il trattamento dei dati personali avviene sia all'interno delle sedi del Titolare sia all'esterno. Nel dettaglio per ciò che concerne:

a) i dati contabili, di sicurezza ed ambiente, della gestione del personale per conto dei clienti, della selezione del personale in proprio e per conto dei clienti, i dati relativi a conteziosi dei degli associati vengono trattati all'interno dell'azienda sui singoli pc degli operatori;
b) I dati di ambiente e sicurezza possono essere trattati anche da consulenti esterni a cui è stato dato incarico;
c) la posta elettronica risulta essere gestita da Unindustria Como con sede in Como a mezzo del servizio di Microsoft 0365 (in cloud);

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

**A – Schedari ed altri supporti cartacei ed elettronici**

I supporti cartacei, ivi inclusi quelli contenenti immagini, sono ordinatamente raccolti in schedari, ovvero nella pratica cui si riferiscono, per essere archiviati, una volta terminato il ciclo lavorativo.
I file di supporto sono archiviati presso i server aziendali e protetti da sistemi di protezione.

**B – Elaboratori in rete con accesso privato**

Per elaboratori in rete con accesso privato si intendono quegli elaboratori, per ciascuno dei quali è identificato uno specifico incaricato, che sono collegati tramite una rete cui possono accedere unicamente i soggetti autorizzati interni all'organizzazione del Titolare.
Il Titolare dispone dell'hardware e software indicato nell'allegato 2.

## CAPITOLO 2 - MANUALE INTERNO DELLA PRIVACY

### 2.1 Responsabile del trattamento

Il Titolare nomina per ciascun anno ovvero fino a revoca espressa il/i Responsabile/i ai sensi del'art. 29 D.Lgs. 196/2003 ed art. 30 del GDPR n. 679/2016, individuandolo/i tra i soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle disposizioni normative in materia. La nomina del/i Responsabile/i e la relativa accettazione avvengono con atto separato, allegato al RPD. La nomina di ciascun Responsabile può riguardare anche soltanto i trattamenti relativi a specifiche aree.[1]

Il Titolare, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni normative, di sicurezza, e delle proprie istruzioni.

Il responsabile attualmente nominato con contratto scritto è il direttore generale dott. Antonello Regazzoni (allegato 3).

Compiti del Responsabile sono:

- Gestire i trattamenti, attenendosi alle istruzioni impartite dal Titolare.
- Supervisionare e provvedere al mantenimento in efficienza delle misure di sicurezza, conformemente a quanto previsto dagli artt. 31 e 33 Dlgs 196/2003 ed art. 30 del GDPR n. 679/2016.
- Garantire il soddisfacimento dei diritti esercitabili dai soggetti interessati, ai sensi degli articoli da 7 a 10 D. lgs. 196/2003 ed art. 17 del GDPR n. 679/2016.
- Aggiornare gli elementi descrittivi del RPD ed il registro di trattamento dei dati.
- Nominare Incaricati del trattamento ai sensi dell'art. 30 D.Lgs. 196/2003.
- Fornire agli Incaricati le indicazioni di carattere operativo necessarie al corretto adempimento dei relativi incarichi.

[1] Nel RPD, per brevità, si farà riferimento al Responsabile, anche se il Titolare può nominarne più di uno. Il termine "Responsabile", pertanto, intende comprendere ogni Responsabile, con riferimento alle relative aree di competenza.

## 2.2 Gli Incaricati del trattamento

Il trattamento dei dati personali può essere effettuato esclusivamente da Incaricati ai sensi dell'art. 30 D.Lgs. 196/2003 (gli "Incaricati") che operano sotto la diretta autorità del Titolare o del Responsabile, attenendosi alle istruzioni impartite.
La designazione degli Incaricati avviene a cura del Titolare o del Responsabile:

- per iscritto, individuando puntualmente l'ambito del trattamento consentito, ovvero
- mediante la documentata preposizione del soggetto ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima.

La lista degli Incaricati ovvero delle unità per le quali è individuato l'ambito di trattamento di dati personali consentito, è allegata al RPD ed è aggiornata a cura del Responsabile (allegato 4).

## 2.3 Disposizioni relative al trattamento dei dati

1. I dati personali oggetto di trattamento sono:
   a) trattati in modo lecito e secondo correttezza;
   b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in termini compatibili con detti scopi;
   c) esatti e periodicamente aggiornati;
   d) pertinenti, completi e non eccedenti le finalità per le quali sono raccolti e trattati;
   e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.
2. I dati segnalati nel Registro di Trattamento dei Dati verranno trattati in conformità alla normativa vigente; il Responsabile fornisce specifiche indicazioni al riguardo, con riferimento alle singole ipotesi.
3. I documenti contenenti dati personali sono custoditi ed archiviati in conformità alle misure di sicurezza di cui al cap. 4 del RPD.

4. Gli strumenti elettronici ed i documenti cartacei contenti dati personali non devono essere lasciati incustoditi e accessibili.
5. In caso di cessazione di un trattamento, i dati sono (i) distrutti, (ii) ceduti ad altro titolare nel rispetto della normativa, (iii) conservati e non destinati alla comunicazione sistematica o alla diffusione.
6. Gli addetti alla gestione e manutenzione del sistema informativo non sono autorizzati ad effettuare alcun trattamento sui dati personali contenuti negli strumenti elettronici, fatta eccezione per i trattamenti di carattere temporaneo strettamente necessari per effettuare la gestione o manutenzione del sistema.

**2.4 Informativa**

1. Ogni trattamento di dati personali da parte del Titolare, del Responsabile, e degli Incaricati, è consentito esclusivamente per lo svolgimento delle funzioni inerenti l'attività aziendale.
2. Il Titolare informa per iscritto, anche tramite il Responsabile o gli Incaricati ed anche tramite il sito aziendale della società (ove possibile), ogni interessato relativamente alle finalità e le modalità del trattamento cui sono destinati i dati; alla natura obbligatoria o facoltativa del conferimento dei dati; alle conseguenze di un eventuale rifiuto di rispondere; ai soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi; ai diritti riconosciuti all'interessato ai sensi dell'art.7 D.Lgs. 196/2003 ed art. 17 del GDPR n. 679/2016; agli estremi identificativi del Titolare e del Responsabile.
2. L'informativa è resa al momento di instaurazione del rapporto, salvo che si renda necessario il rinnovamento della stessa per intervenute modifiche del trattamento comunicato.

**2.5 Consenso, comunicazione e diffusione**

1. Il consenso al trattamento di dati personali è disciplinato da quanto disposto dall'art. 7 del GDPR n. 679/2016.

2. Il consenso è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, viene documentato per iscritto, ed è resa all'interessato l'informativa di cui al punto 2.4 nei termini di legge.
3. Quando il trattamento riguarda dati sensibili, il consenso è manifestato in forma scritta o equiparata in via digitale.
4. Il consenso non è richiesto nei casi di cui all'art.24 D.Lgs. 196/2003 e negli altri eventuali casi di legge.
5. La comunicazione e la diffusione sono vietate: (i) in caso di divieto disposto dal Garante per la Protezione dei Dati Personali o dall'autorità giudiziaria, (ii) in riferimento a dati personali dei quali è stata ordinata la cancellazione, (iii) quando è decorso il periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e trattati, (iv) per finalità diverse da quelle indicate nell'informativa di cui al punto 2.4.
6. E' ammessa la comunicazione o diffusione di dati qualora richieste, in conformità alla legge, da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici competenti a norma di legge per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.

**2.6 Diritti degli interessati**

1. Conformemente alle previsioni di cui all'art. 7 D.Lgs. 196/2003 ed all'art. 15 del GDPR n. 679/2016, ogni interessato ha diritto di ottenere conferma dell'esistenza o meno di dati personali gestiti dalla Titolare, e la loro comunicazione. Inoltre, ha diritto di ottenere l'indicazione dell'origine dei dati personali, delle finalità e modalità del trattamento, della logica applicata in caso di trattamento effettuato mediante strumenti elettronici, degli estremi identificativi del Titolare e del Responsabile, dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di Incaricati. L'interessato ha infine diritto di ottenere l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati; la cancellazione, la trasformazione in forma anonima o il blocco dei dati qualora questi fossero trattati in violazione di legge; l'attestazione che le operazioni di cui sopra sono state portate a conoscenza di coloro cui i dati sono stati

comunicati o diffusi, eccettuato il caso in cui tale adempimento sia impossibile o comporti un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

2. Nel caso di esercizio da parte di un interessato dei diritti di cui all'articolo 7 D.Lgs. 196/2003 ed art. 17 del GDPR n. 679/2016, ne viene prontamente informato il Responsabile, il quale verifica l'identità dell'interessato sulla base di idonei elementi di valutazione. Qualora per conto dell'interessato agisse una persona terza, alla stessa è richiesto di allegare copia della procura, ovvero della delega sottoscritta e unitamente a copia di un documento di riconoscimento dell'interessato. Se l'interessato è una persona giuridica, un ente od un'associazione, la richiesta deve essere avanzata dal legale rappresentante o da altra persona legittimata allo scopo.
3. I dati richiesti sono estratti a cura del Responsabile o degli Incaricati e possono essere comunicati al richiedente anche oralmente, ovvero offerti in visione mediante strumenti elettronici. Se vi è richiesta in tal senso, si provvede alla trasposizione dei dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica; nel caso in cui l'estrazione dei dati risulti particolarmente difficoltosa, il riscontro può avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti.

   Salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprende tutti i dati personali che riguardano l'interessato comunque trattati dal Titolare.

   La comunicazione dei dati non comprende i dati personali relativi a terzi, salvo che la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato.

   Qualora non risulti confermata l'esistenza di dati riguardanti l'interessato, può essere richiesto un contributo spese non eccedente i costi effettivamente sopportati per la ricerca effettuata.

### 2.7 Formazione

Il Titolare prevede espressamente lo svolgimento di appositi **interventi formativi nei confronti degli Incaricati del trattamento**, finalizzati in particolare ad illustrare:

- profili della disciplina sulla protezione dei dati personali e delle conseguenti responsabilità che ne derivano;
- rischi che incombono sui dati personali;
- misure per prevenire eventi dannosi;
- aggiornamento sulle misure di sicurezza adottate dal Titolare.

Tali interventi formativi hanno luogo al momento dell'ingresso in servizio, in occasione di cambiamenti di mansioni implicanti modifiche rilevanti rispetto al trattamento di dati personali, nonché in occasione dell'introduzione di nuovi strumenti che implichino modifiche rilevanti nel trattamento di dati personali.

Gli interventi formativi sono curati dal Responsabile, che a tal fine può avvalersi anche di soggetti esterni.

## 3. ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

La mappatura dei rischi relativi al trattamento di dati da parte del Titolare è effettuata tenendo in considerazione (i) i rischi relativi ai dati in funzione della relativa tipologia, e (ii) i rischi relativi alle specifiche modalità di trattamento adottate.

### *3.1. Rischi in funzione della tipologia dei dati*

Il grado di rischio dipendente dalla tipologia dei dati trattati dal Titolare viene qui definito combinando l'intensità del rischio (derivante dal possibile interesse da parte di terzi ad accedervi) con la pericolosità del trattamento (valutata in funzione del danno per il soggetto cui i dati si riferiscono in caso di accesso illegittimo).

| | | | | |
|---|---|---|---|---|
| **INTENSITA' DEL RISCHIO**<br><br>**(INTERESSE PER I TERZI)** | **ALTO** | • Anagrafica fornitori<br>• Rapporti contrattuali in essere con fornitori | | • Coordinate bancarie fornitori<br>• Coordinate bancarie clienti<br>• Redditi / coordinate bancarie dipendenti<br>• Visite mediche aziendali<br>• Adesione a sindacati<br>• Adesione a scioperi<br>• Stato di salute permanente dipendenti<br>• Assenze dipendenti<br>• Stato civile dipendenti<br>• Posizioni di insolvenza dei dipendenti |

| | | | | |
|---|---|---|---|---|
| | **MEDIO** | • Anagrafica clienti | • Dati anagrafici e titoli dipendenti<br>• Certificati medici dipendenti | • Dati commerciali |
| | **BASSO** | • Ferie dipendenti<br>• Dati candidati | | |
| | | **BASSO** | **MEDIO** | **ALTO** |
| | | **PERICOLOSITA' DEL TRATTAMENTO (DANNO PER L'INTERESSATO)** | | |

In relazione a quanto disposto dal GDPR n. 679/2016 la società dovrà porre in essere misure di tutela per i dati individuati con pericolosità ALTA del trattamento in danno all'interessato.

### 3.2. Rischi in funzione delle modalità di trattamento adottate

I rischi relativi alle specifiche modalità di trattamento adottate, vengono qui valutati sulla base degli strumenti impiegati per il trattamento, le cui componenti di rischio possono essere sinteticamente suddivise come segue.

1. Rischio di area, dipendente dal luogo dove gli strumenti sono ubicati. Tale rischio è legato sostanzialmente al verificarsi di eventi distruttivi (incendi, allagamenti, ecc.);
2. Rischio di guasti tecnici, particolarmente rilevante relativamente agli strumenti elettronici.
3. Rischio di penetrazione nelle reti di comunicazione e negli archivi.
4. Rischio legato ad atti volontari o ad errori umani da parte del personale o di terzi ( fornitori).

Nella tabella che segue sono evidenziati i fattori di rischio cui sono soggetti gli strumenti con cui l'organizzazione procede al trattamento dei dati personali.
Il simbolo **B**, posto nella casella di intersezione, significa che l'esposizione al rischio appare modesta; il simbolo **M** significa che l'esposizione al rischio appare riconducibile alla media, il simbolo **A** significa che l'esposizione al rischio appare elevata

| **TIPI DI DATI TRATTATI** | | | | |
|---|---|---|---|---|
| Rischio d'area, legato al verificarsi di eventi distruttivi | M | M | M | |
| Rischio d'area, legato all'accesso non autorizzato nei locali | M | B | B | |
| Rischio di guasti tecnici di hardware, software e supporti | - | M | M | |
| Rischio di penetrazione logica nelle reti di comunicazione | - | B | M | |

| | | | | |
|---|---|---|---|---|
| Rischio legato ad atti di sabotaggio e ad errori umani | M | M | M | |
| | **S** | **Enr** | **Epv** | **Epb** |
| | STRUMENTI UTILIZZATI | | | |

Legenda degli strumenti utilizzati per il trattamento:

**S**: Schedari ed altri supporti cartacei

**Enr**: Elaboratori non in rete

**Epv**:Elaboratori in rete con accesso privato

**Epb**: Elaboratori, in rete con accesso pubblico

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

Nel presente capitolo sono descritte le misure atte a garantire:

- la protezione delle aree e dei locali, nei quali si svolge il trattamento dei dati personali, nonché la corretta archiviazione e custodia di atti, documenti e supporti contenenti dati personali;
- la sicurezza logica, nell'ambito dell'utilizzo degli strumenti elettronici.

### 4.1 Protezione di aree e locali; archiviazione e custodia

Per quanto concerne il rischio d'area legato ad eventi di carattere distruttivo, i locali del Titolare sono protetti da dispositivi antincendio, a norma di legge.

Per quanto riguarda le misure atte ad impedire gli accessi non autorizzati ai locali nei quali si svolge il trattamento, sono disposti i seguenti presidi:

- Presenza di un sistema anti-intrusione.
- Specifico obbligo di vigilanza da parte del personale interno.
- Espresso obbligo per gli Incaricati di non lasciare incustoditi gli Archivi. In particolare, nei locali dove vengono trattati dati personali dovrà essere sempre presente almeno un Incaricato o il Responsabile, durante l'orario lavorativo; in caso di impossibilità, detti locali devono essere chiusi a chiave. Detti locali devono essere chiusi a chiave al termine della giornata lavorativa.
- Armadi, cassetti e simili nei quali sono conservati dati sensibili, anche su supporto informatico (CD-Rom, periferica USB), devono essere chiusi a chiave.
- Presenza di casseforti nelle quali sono custoditi i dati cartacei considerati a maggiore rischio.
- Obbligo per gli Incaricati di riporre la documentazione contenente dati personali su supporto non elettronico negli Archivi al termine delle operazioni affidate.

Il Titolare ed il Responsabile individuano le procedure più idonee finalizzate alla conservazione degli atti – laddove necessario – in archivi ad accesso selezionato, nonché alla identificazione degli Incaricati che vi accedono.

Su base annua, il Responsabile procede all'aggiornamento dell'ambito di trattamento consentito ai singoli Incaricati o alle unità organizzative.

Sono previsti i seguenti interventi:

- Specifica formazione del personale, con particolare riferimento agli Incaricati.
- Verifica da parte del Responsabile del rispetto delle disposizioni del Titolare in materia di trattamento dei dati.

### 4.2 Le misure logiche di sicurezza

Per i trattamenti effettuati con strumenti elettronici (elaboratori, programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato), sono adottati i seguenti presìdi:

- Sistema di autenticazione informatica, che permette l'accesso ad ogni elaboratore esclusivamente ai soggetti autorizzati.
- Sistema di autorizzazione, che circoscrive le tipologie di dati cui gli Incaricati possono accedere, ed relativi i trattamenti .
- Sistema di protezione degli elaboratori e dei dati ivi contenuti da malfunzionamenti, attacchi informatici e programmi contenenti *virus.*
- Sistema di custodia ed utilizzo dei supporti rimovibili (CD-Rom,USB ecc.), nei quali siano contenuti dati personali.
- Sistema anti – intrusione Firewall

Qualora le misure minime siano adottate avvalendosi di soggetti esterni alla struttura del Titolare, l'installatore rilascerà una descrizione scritta dell'intervento effettuato che ne attesti la conformità alle disposizioni del Disciplinare Tecnico allegato al D.Lgs. 196/2003.

#### *4.2.1 Autenticazione*

L'accesso al trattamento è soggetto alla previa autenticazione informatica del soggetto operante tramite utilizzo di apposite credenziali di autenticazione ("Credenziali").

- Le Credenziali consistono in un codice per l'identificazione dell'Incaricato tramite una parola chiave, composta da almeno otto caratteri, riservata conosciuta solamente dal

medesimo ovvero in un dispositivo di autenticazione in possesso e uso esclusivo dell'Incaricato. La parola chiave non contiene riferimenti agevolmente riconducibili all'Incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. Il sistema informatico dell'azienda è definito in modo tale da permettere al Responsabile l'accesso ai files contenenti dati personali.

- In caso di trattamento di dati sensibili e/o dati giudiziari la parola chiave è modificata ogni tre mesi.
- Ad ogni Incaricato sono assegnate o associate individualmente una o più Credenziali per l'autenticazione. La parola chiave, o altro codice per l'identificazione, non possono essere assegnati ad altri Incaricati, neppure in tempi diversi. Le Credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate. Le Credenziali sono disattivate anche in caso di perdita della qualità che consente all'Incaricato l'accesso ai dati personali.
- Gli Incaricati sono tenuti ad adottare le necessarie cautele per assicurare la segretezza della componente riservata della Credenziale e la diligente custodia degli eventuali dispositivi in loro possesso ed uso esclusivo.
- Gli Incaricati non devono lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento. Qualora si renda necessaria una interruzione, detto strumento deve essere "ibernato".
- In caso di prolungata assenza o impedimento dell'Incaricato, qualora si renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, la disponibilità dei dati è assicurata dal Responsabile, con le modalità ritenute più opportune, che informa tempestivamente l'Incaricato dell'intervento effettuato.

Le disposizioni sul sistema di autenticazione non si applicano ai trattamenti di dati personali destinati alla diffusione.

*4.2.2. Autorizzazione:*

- Ogni Incaricato è abilitato a trattare esclusivamente i dati per i quali ha ricevuto l'incarico. Le autorizzazioni all'accesso vengono rilasciate e revocate dal Titolare ovvero dal

Responsabile. Il profilo autorizzativo può essere definito per ogni singolo Incaricato, ovvero essere impostato per classi omogenee di Incaricati.

- Gli addetti alla gestione e manutenzione del sistema informativo non sono autorizzati ad effettuare alcun trattamento sui dati personali contenuti negli strumenti elettronici, fatta eccezione per i trattamenti di carattere temporaneo strettamente necessari per effettuare la gestione o manutenzione del sistema.
- Con cadenza periodica, almeno annuale, il Responsabile procede all'aggiornamento dell'individuazione dell'ambito del trattamento, nonché alla verifica della sussistenza delle condizioni per la conservazione dei profili di autorizzazione in capo agli Incaricati ed agli addetti alla manutenzione e gestione degli strumenti elettronici

Le disposizioni sul sistema di autorizzazione non si applicano ai trattamenti di dati personali destinati alla diffusione.

*4.2.3 Protezione degli elaboratori e dei dati ivi contenuti*

Per quanto riguarda la protezione degli elaboratori e dei dati ivi contenuti da malfunzionamenti, accessi non consentiti, e virus informatici, vengono adottate le seguenti misure.

- I dati personali sono protetti contro il rischio di intrusione e dell'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, tramite l'adozione di programmi "antivirus", che sono sottoposti ad aggiornamento almeno semestrale.
- I dati personali sono protetti contro il rischio di accesso abusivo di cui all'articolo 615-*ter* del codice penale (introduzione abusiva in un sistema informatico o telematico protetto da misure di sicurezza, ovvero mantenimento nello stesso contro la volontà espressa o tacita di chi ha il diritto di escluderne i terzi), mediante l'impiego di idonei strumenti elettronici ("*firewall*"), sottoposti ad aggiornamento almeno semestrale.

*4.2.4 Custodia ed utilizzo dei supporti rimovibili contenenti dati personali.*

Per quanto concerne i supporti rimovibili (es. CD-Rom, periferiche USB) contenenti dati personali, agli Incaricati è fatto obbligo di custodire ed utilizzare detti supporti in modo tale da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti. In particolare, essi devono essere conservati in cassetti o armadi chiusi a chiave e, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi, cancellati in modo definitivo.

Sono previsti i seguenti interventi:

- Manutenzione ed aggiornamento dei programmi antivirus.
- Manutenzione ed aggiornamento dei programmi "firewall".
- Verifica da parte del responsabile del rispetto delle disposizioni del Titolare in materia di trattamento dei dati.

## 5. Criteri e modalità di ripristino dei dati

Per i dati trattati con strumenti elettronici, è previsto il salvataggio di una copia di backup di tutti i dati contenuti su tutti i server. Dette copie sono effettuate su NAS con cadenza quotidiana e mensile, e custodite a cura del Responsabile in luoghi protetti.
I dati trattati sugli Elaboratori sono salvati con frequenza almeno giornaliera.

Il ripristino della disponibilità dei dati e dei sistemi è ulteriormente garantito tramite apposite intese con il soggetto incaricato della gestione del sistema.

## 6.Data Breach

La società, ai sensi dell'art. 33 del GDPR n. 679/2016, ha provveduto ad implementare una propria procedura interna per disciplinare l'obbligo di comunicazione al Garante della Privacy nonché /all'interessato in caso di avvenuto data breach.

## 1. Affidamento di dati personali all'esterno

Nei casi in cui i trattamenti di dati personali vengano affidati, in conformità a quanto previsto dal D.Lgs. 196/2003, all'esterno della struttura del Titolare, si adottano i seguenti criteri, atti a garantire che il soggetto destinatario adotti misure di sicurezza conformi a quelle minime, previste dagli articoli da 33 a 35 del D.Lgs. 196/2003 e dal Disciplinare Tecnico, allegato sub b) al Decreto medesimo.

In particolare, la gestione del server esterno avviene in conformità alle misure di sicurezza adottate dal fornitore del servizio, relativamente alle quali il Titolare esercita la supervisione tramite la consegna di copia di un Documento attestante la propria Sicurezza dei dati, nonché dell'ulteriore documentazione ritenuta necessaria od opportuna.

Per la generalità dei casi, in cui il trattamento di dati personali, di qualsiasi natura, venga affidato all'esterno della struttura del Titolare, sono impartite istruzioni al terzo destinatario di rispettare quanto prescritto per il trattamento dei dati personali dal Dlgs 196/2003, ovvero dalla direttiva 95/46/CE se il terzo destinatario non è europeo in conformità a quanto disposto dal GDPR n. 679/2016.
Nei casi in cui il trattamento affidato all'esterno abbia per oggetto dati sensibili o giudiziari, si procede alla stipula di apposite clausole contrattuali con il destinatario, che disciplinino gli aspetti legati alla gestione dei dati personali.

Nell'ipotesi in cui il trattamento, di dati sensibili o giudiziari, avvenga con strumenti elettronici, si esige inoltre che il destinatario rilasci la dichiarazione di avere redatto un proprio documento programmatico sulla sicurezza, col quale abbia recepito le disposizioni normative in tema di misure minime di sicurezza.

## 7. Dichiarazioni d'impegno e firma

Il presente Regolamento di Protezione dei Dati è stato redatto, ai sensi dell'art. 34 del D.Lgs. 196/2003 e della regola 19 allegato B al codice dal Titolare ed in conformità a quanto disposto dal GDPR n. 679/2016.
Lo stesso è portato a conoscenza di tutti gli Incaricati.
Rimane a disposizione degli organi competenti presso il Titolare.

Como, lì 14 maggio 2018

Firma del legale rappresentante _____
TITOLARE DEL TRATTAMENTO DEI DATI.

**Allegati**

Allegato 1 registro dei trattamenti;
Allegato 2 elenco software e hardware;
Allegato 3: nomina respondabile;
Allegato 4: elenco incaricati;
Allegato 4 bis elenco incaricati a tempo determinato.