L'AQUILONE COOPERATIVA SOCIALE
Via Manara Valgimigli, 1 - 24020 Vilminore di Scalve (BG)

Politica aziendale per la protezione dei dati personali, al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche
Regolamento UE 2016/679 – GDPR

1. SCOPO E AMBITO DI APPLICAZIONE

Scopo della presente è quello di descrivere i principi generali di sicurezza e gli obblighi di riservatezza delle informazioni e dei dati personali definiti dal Titolare del trattamento, garantire e assicurare a tutti i soggetti coinvolti nell'ambito del trattamento dei dati un efficiente e sicuro sistema di gestione delle procedure e dei processi per la sicurezza dei dati personali, nel rispetto dei diritti e delle libertà fondamentali delle persone, in ottemperanza al Regolamento Europeo 2016/679, d'ora in avanti GDPR.
La politica per la protezione dei dati personali si applica a tutti gli Utenti che collaborano alla gestione delle informazioni nonché a tutti i processi e risorse coinvolte nella progettazione, realizzazione, avviamento ed erogazione continuativa nell'ambito dell'attività svolta.

2. DESCRIZIONE

Obiettivi perseguiti

Il titolare del trattamento intende perseguire obiettivi di sicurezza delle informazioni, dei dati personali, della struttura tecnologica, fisica, logica ed organizzativa e della loro gestione. Questo significa raggiungere e mantenere un sistema di gestione sicura delle informazioni, attraverso il rispetto dei principi previsti dagli articoli 5 e 6 del GDPR:

- Liceità, correttezza, trasparenza;
- Garanzia rispetto alla gestione e raccolta dei dati per le sole finalità contrattuali, determinate, esplicite e legittime; successivamente i dati sono trattati in modo che non Vi sia incompatibilità con tali finalità. Tali garanzie sono applicate e verificate anche a cascata nei confronti degli eventuali subfornitori;
- I dati raccolti sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (principio di "minimizzazione dei dati");
- I dati raccolti sono esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati ("esattezza");
- I dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
- I dati sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche ed organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali "principio di integrità e riservatezza";
- Assicurare che i dati personali siano accessibili solamente ai soggetti e/o alle categorie degli stessi debitamente autorizzati;
- Salvaguardare la consistenza dell'informazione da modifiche non autorizzate;
- Assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetturali associati in riferimento ai ruoli e mansioni ricoperti;
- Assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati;
- Garantire l'affidabilità dei canali di provenienza delle informazioni;
- Garantire la protezione ed il controllo dei dati personali.

Piano di formazione

Considerato che il GDPR all'articolo 29 prevede che tutte le persone sotto l'autorità del titolare, addetti o incaricati, debbano essere debitamente istruiti e quindi formati sui compiti, le responsabilità e le modalità per l'effettuazione delle operazioni di trattamento dei dati, nonché si debbano impegnare alla riservatezza, Il titolare del trattamento ha redatto un piano di formazione sulla base dell'erogazione dei servizi, dei ruoli e mansioni interne, dell'attività esercitata, degli specifici trattamenti dati ed i rischi connessi.

Gestione fornitori

I principi e le garanzie sono verificati al momento della scelta di ogni nostro fornitore. Viene inoltre monitorato sistematicamente lo stato di implementazione di tali garanzie.

3. POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

Adempimenti e procedure applicate alle aziende clienti

• La verifica dei dati che saranno oggetto di trattamento con identificazione delle varie tipologie di dati e delle categorie di appartenenza. La verifica della finalità di ogni trattamento e della base giuridica sul quale ciascuno di essi si fonda, anche al fine di rendere adeguata informativa ai soggetti interessati, come previsto dagli artt. 13 e 14 del GDPR;

• La predisposizione della/delle informativa/e (o il loro aggiornamento), che deve/devono essere fornita/e agli interessati nel rispetto di tutti gli elementi indicati agli artt. 13 e 14 del GDPR. In particolare gli interessati dovranno essere messi a conoscenza dei diritti che il Regolamento riconosce loro (diritto di accesso, diritto all'oblio, diritto di rettifica, diritto di limitazione e di opposizione al trattamento, diritto alla portabilità dei dati); le informative per i soggetti interessati ai trattamenti dati di cui il cliente è titolare del trattamento sono fornite dal cliente se nei software o servizi sviluppati o configurati è prevista la raccolta di dati;

• La predisposizione del registro delle attività di trattamento dei dati personali di cui all'art. 30 del GDPR;

• L'instaurazione di una procedura da adottare in caso di eventuali violazioni dei dati (c.d. Data Breach di cui agli articoli 33 e 34 del GDPR), ad esempio al verificarsi di una divulgazione (intenzionale o meno), della distruzione, della perdita, della modifica o dell'accesso non autorizzato ai dati personali oggetto di trattamento. Il GDPR prevede infatti degli specifici adempimenti nel caso in cui si verifichi una violazione di tal genere, a causa di un attacco informatico, di un accesso abusivo o di un incidente. In questi casi il GDPR impone, come previsto dall'art. 33, in capo al Titolare del trattamento l'obbligo di comunicare all'autorità di controllo l'avvenuta violazione entro 72 ore (o comunque senza ritardo). Nel caso in cui la violazione verificatasi faccia presumere che vi sia anche un elevato e attuale pericolo per i diritti e le libertà degli interessati, anche questi ultimi dovranno essere direttamente informati senza ritardo di quanto successo;

• All'art. 35 del GDPR, si configura, in capo al Titolare del trattamento, l'obbligo di procedere ad una valutazione d'impatto sulla protezione dei dati nel caso in cui un tipo di trattamento, anche in considerazione della natura, dell'oggetto, del contesto e delle finalità del trattamento stesso, presenti un rischio elevato per i diritti e le libertà delle persone fisiche. Si precisa che il GDPR non sancisce un vero e proprio obbligo di svolgimento della valutazione d'impatto, ma si ricorda che il Regolamento prevede un generale obbligo, in capo al Titolare del trattamento, di attuare le misure idonee al fine di gestire adeguatamente i rischi per i diritti e le libertà degli interessati che possono derivare dal trattamento dei loro dati. Si è reso quindi opportuno predisporre il Documento di Analisi e Valutazione del Rischi per la Protezione dei Dati

• Agli articoli 37 – 38 e 39 viene introdotto un altro adempimento richiesto al Titolare del trattamento che consiste nella designazione del Responsabile della protezione dei dati definito altresì Data Protection Officer.

4.ISTRUZIONE DEGLI UTENTI

Particolare importanza viene attribuita alle procedure del Sistema di Gestione per la Protezione dei dati personali, indicate nelle istruzioni e formazione che dovranno essere fornite al personale ed alle quali vi è l'obbligo di attenersi scrupolosamente.
Vi è obbligo inoltre di prendere visione dei nominativi del personale autorizzato a trattare i dati relativi all'ambito assegnato, siano essi Titolari, responsabili o incaricati (Come definiti nell'organigramma).
È stata promossa una Policy Interna GDPR *(Regole di condotta ed obblighi in relazione all'uso degli strumenti di lavoro)*, il personale è tenuto a prenderne visione ed a comunicare ai suoi referenti eventuali inesattezze.

5. RESPONSABILITÀ DELLA POLITICA DI SICUREZZA DELLE INFORMAZIONI

Il "titolare del trattamento" è responsabili del sistema di gestione sicura delle informazioni, in coerenza con l'evoluzione del contesto aziendale e di mercato, valutando eventuali azioni da intraprendere a fronte di eventi come:

- Evoluzioni significative del business;
- Nuove minacce rispetto a quelle considerate nell'attività di analisi del rischio;
- Significativi incidenti di sicurezza;
- Evoluzione del contesto normativo o legislativo in materia di trattamento sicuro delle informazioni;

Periodicamente o all'occorrenza dovrà essere svolto un riesame per la verifica dell'efficienza e dell'efficacia, nonché dell'adeguatezza delle misure tecniche/organizzative applicate, nel rispetto ed al fine ultimo della protezione dei dati, diritti e libertà fondamentali delle persone.

Vilminore di Scalve, 09/10/2018

Per approvazione
Il Legale Rappresentante

_____