DICHIARAZIONE DI CONFORMITÀ AL GDPR

Regolamento generale sulla protezione dei dati

Il Regolamento generale sulla protezione dei dati, o GPDR, è un regolamento dell'Unione Europea che stabilisce un nuovo quadro normativo per la protezione dei dati personali dei cittadini dell'UE. Il GDPR rappresenta la parte più significativa della legislazione europea in materia di protezione dei dati dopo la Direttiva sulla protezione dei dati dell'UE del 1995.

Il GDPR ha l'obiettivo di armonizzare e portare le leggi sulla protezione dei dati in tutta Europa al passo con i rapidi cambiamenti tecnologici avvenuti negli ultimi due decenni. Il regolamento si basa su precedenti quadri giuridici europei, compresa la Direttiva sulla protezione dei dati dell'UE, introducendo nuovi obblighi e responsabilità per le organizzazioni che trattano dati personali e nuovi diritti per le persone in merito ai propri dati personali. Le organizzazioni con sede nell'UE, così come le organizzazioni che trattano dati personali di residenti nell'UE, sono tenute a rispettare il GDPR.

OPENTUR SRL verso la conformità con il GDPR

OPENTUR SRL s'impegna a garantire la conformità con il GDPR. Il rispetto della privacy e della sicurezza è un aspetto vitale della nostra attività sin dall'inizio; la nostra attenzione al trattamento e alla protezione dei dati è rimasta una priorità.

Il percorso di OPENTUR SRL verso la conformità con il GDPR è iniziato prima della scadenza “naturale” della normativa. Il nostro primo passo è stato formare un team trasversale di specialisti della protezione dei dati composto da consulenti legali, professionisti della sicurezza e della conformità. Il nostro team ha quindi completato una valutazione completa delle nostre attuali pratiche di sicurezza e protezione dei dati rispetto alle disposizioni del GDPR. Il nostro prossimo passo è stato eseguire una valutazione delle nostre attività di trattamento dei dati personali e tracciare il ciclo di vita dei dati personali attraverso i nostri sistemi. A volte queste operazioni vengono definite come "mapping dei dati" e integrano le valutazioni dell'impatto sulla protezione dei dati.

Il metodo di lavoro è esplicitamente estratto dalle linee guide del Garante della privacy del Regno Unito (Information Commissioner Officer) per quanto riguarda il modello organizzativo del ciclo di “vita” dell’adeguamento al GDPR. Fatte salve le richieste esplicite contenute nel Regolamento Europeo (in particolare i principi di privacy by design e default, le informative e la raccolta del consenso, le policy interne e di data breach), il modello vuole essere un percorso di miglioramento aziendale.

La nostra organizzazione ha inoltre deciso di adottare tutte le misure minime contenute nel D.lgs. 196/03, Testo Unico sulla Sicurezza dei Dati. Il modello di analisi degli eventi infine è ispirato al modello presentato nell’allegato B, del Testo Unico, al punto 19.3.

Da allora, abbiamo continuato a sviluppare le procedure interne in essere per garantire il rispetto dei principi di responsabilità ai sensi del GDPR.

CONTROLLI: LE NOSTRE PRASSI INTERNE

Adottiamo misure esaustive per proteggere la nostra infrastruttura, la nostra rete e le nostre applicazioni, formare i dipendenti sulle pratiche in ambito di sicurezza e privacy e costruire una cultura in cui conquistare la fiducia dei clienti è la massima priorità. Di seguito sono descritte in dettaglio alcune delle nostre misure di controllo

Formazione

Parte della garanzia di protezione dei dati personali dei nostri utenti consiste nel diffondere e favorire la conoscenza delle nozioni di sicurezza e privacy. A questo proposito, ai dipendenti viene richiesta l'accettazione delle norme di sicurezza, incluse le Norme sulla privacy dei dati, prima ancora di ottenere l'autorizzazione ad accedere ai sistemi. Inoltre, i dipendenti partecipano a corsi di formazione obbligatori sulla sicurezza e sulla privacy per i nuovi assunti, oltre alla formazione annuale di follow-up e a una sensibilizzazione continua su tali temi mediante e-mail informative, conferenze, presentazioni e risorse disponibili sulla rete Internet.

Richieste di accesso a dati personali

Gli utenti hanno anche la possibilità di richiedere l'accesso o la cancellazione di altri dati personali raccolti su di loro. Ulteriori informazioni su questo processo sono disponibili facendo richiesta.

Soggetti terzi che collaborano con OPENTUR SRL

La nostra azienda gestisce in prima persona la maggior parte delle attività relative alla fornitura dei propri servizi; tuttavia, si avvale di alcune terze parti fidate in relazione ai servizi offerti, quali fornitori di assistenza clienti e servizi IT, che accedono alle tue informazioni solo per eseguire attività per nostro conto in conformità con le nostre Norme sulla privacy.

OPENTUR SRL ne assicura il trattamento in conformità con le proprie istruzioni. Ogni parte terza passa attraverso un rigoroso processo di controllo, incluse verifiche in materia di sicurezza e revisioni contrattuali periodiche, per valutarne la di rispettare i nostri impegni di protezione dei dati

Trasferimento internazionale di dati

OPENTUR SRL fa affidamento su un'ampia gamma di meccanismi legali per il trasferimento internazionale di dati personali dall'UE a Paesi Extra UE (Stati Uniti, per esempio per servizi Cloud). Oltre a ciò, offriamo anche solide garanzie contrattuali sulla privacy dei propri servizi e ci affidiamo a clausole contrattuali di tipo UE per il trasferimento internazionale di dati.

APPENDICE: MODELLO ORGANIZZATIVO

FASE 1: GESTIONE E SICUREZZA DELLE INFORMAZIONI ORGANIZZATIVE

1.1 Gestione del rischio

L'azienda ha individuato un processo per identificare, valutare e gestire i rischi legati alla sicurezza delle informazioni, e garantisce che i rischi sulla sicurezza delle informazioni vengano valutati e gestiti correttamente. Prima di stabilire il livello di protezione necessario l'azienda, ha controllato i dati personali che raccoglie e tratta in modo da valutare i rischi legati a queste informazioni.

1.2 Politica di sicurezza: aiutare il management a rilasciare una Information Security Policy

Abbiamo pubblicato un'informativa sulla sicurezza delle informazioni approvata anche dai vertici aziendali e offriamo orientamento e supporto su tematiche legate alla sicurezza delle informazioni in base alle esigenze aziendali, alle leggi e regolamenti in vigore. L'informativa consente di affrontare in modo coerente i rischi legati alla sicurezza e fa parte di una politica generale di protezione dei dati personali

1.3 Responsabilità della sicurezza dell'informazione: definire e stabilire un quadro di gestione per coordinare e rivedere l'implementazione della sicurezza delle informazioni

L'azienda ha definito e assegnato le responsabilità legate alla sicurezza delle informazioni e ha individuato chi si occuperà del coordinamento e revisione dell'implementazione dell'informativa sulla sicurezza dei dati.

1.4 Outsourcing: consulenza e revisione degli accordi con fornitori di servizi di terze parti.

L'azienda ha sottoscritto accordi con fornitori di servizi di terze parti che prevedono anche condizioni di sicurezza adeguate al trattamento dei dati personali. In questo modo l'azienda può garantire la protezione dei dati personali accessibili da fornitori terzi. Poiché oggi molte imprese esternalizzano alcuni o tutti i processi di elaborazione dati a servizi hosting (inclusi i cloud), cerchiamo di assicurarci del fatto che questi "processori di dati" trattino le informazioni in modo sicuro.

1.5 Gestione degli incidenti: stabilire un processo per segnalare e recuperare dalle violazioni della sicurezza dei dati.

L'azienda ha individuato un processo adeguato a segnalare e recuperare le informazioni in caso di una violazione della sicurezza dei dati. Possiamo garantire la gestione adeguata delle violazioni alla sicurezza dei dati, inclusa la comunicazione di eventi che mettono a rischio la sicurezza delle informazioni. Le violazioni della sicurezza dei dati possono derivare da un furto, un attacco ai sistemi, l'uso non autorizzato di dati personali da parte di un membro dello staff, da perdita accidentale o guasto di una apparecchiatura.

FASE 2: CONSAPEVOLEZZA DEL PERSONALE SULLA SICUREZZA DELLE INFORMAZIONI

2.1 Formazione e sensibilizzazione del personale anche tramite campagne interne di promozione

L'azienda organizza corsi di formazione sulla sicurezza dei dati, inclusi i corsi dedicati al personale. Ci assicuriamo che dipendenti e fornitori rispettino e siano consapevoli delle loro responsabilità in materia di sicurezza dei dati. Il personale con responsabilità specifiche in materia di sicurezza o con accesso privilegiato ai sistemi di sicurezza aziendali è adeguatamente formato e qualificato.

FASE 3: SICUREZZA FISICA

3.1 *Protezione edifici e locali fisici*

L'azienda ha individuato determinati controlli di accesso per limitare l'accesso a locali e attrezzature, in modo da impedire l'accesso fisico, il danneggiamento e l'interferenza con i dati personali.

Misure fisiche in atto negli uffici

Nella "Struttura" sono attive le seguenti misure di sicurezza relative alla intera struttura, per contrastare le minacce e i possibili impatti:

Accessi dall'esterno	Custode - Antifurto - Sbarre alle finestre - Allarme Vigilanza - Cancelli - Porte con serrature - Serrande
Incendio	estintori - Addetti antincendio con corso
Guasto impianto elettrico	Gruppo i continuità - Messa a terra con revisione - Revisione periodica
Guasto impianto condizionamento	Contratto di assistenza - Impianto di condizionamento
Accessi interni	Uffici presidiati - armadi chiusi a chiave - cassettiera con serratura
Perdita o distruzione dati	Procedure Disaster Recovery - Pianificazione backup

3.2 *Memorizzazione sicura*

L'azienda ha sottoscritto accordi di archiviazione e memorizzazione dei dati sicuri per proteggere i dati e le attrezzature, in modo da cercare di impedire la perdita, il danneggiamento o il furto dei dati personali. Stiamo cercando di fare in modo che tutto il personale adotti misure di sicurezza come chiudere a chiave o mettere in un luogo sicuro documenti cartacei e dispositivi mobili quando non sono in uso.

3.3 *Smaltimento sicuro*

L'azienda ha individuato un processo per cancellare in modo sicuro i dati e le attrezzature quando non sono più necessari. Riteniamo che importante che tutto il personale disponga di attrezzature che memorizzano i dati personali in modo sicuro.

FASE 4: SICUREZZA DEL COMPUTER E DELLA RETE

Nelle infrastrutture IT sono attive le seguenti misure di sicurezza relative alle interconnessioni di rete nella rete locale, per contrastare le minacce e i possibili impatti sulla sicurezza del dato.

Furti	Vedere rischi fisici
Danni dall'esterno	Antifurto
Guasto tecnico	Apparecchiature di scorta - Duplicazione componenti Hw
Errori operativi	Pianificazione backup - Procedure automatizzate - Formazione addetti backup
Carenza di personale	Procedure predefinite - Figure ridondanti

Sono state analizzate le apparecchiature elettroniche che sono coinvolte nelle operazioni di trattamento. Misure per contrastare le minacce e i possibili impatti comuni alle risorse Hardware

Errori operativi	Apparecchiature comuni - Apparecchiature di scorta
Errori di funzionamento	Manutenzione

Stazioni di lavoro personali

Nella “Struttura” sono attive le seguenti misure di sicurezza relative alle stazioni di lavoro personali, per contrastare le minacce e i possibili impatti delle schede “Accesso – stazioni di lavoro”

Introduzione di virus o altro	Antivirus - Antispam - Anti malware - OS Update - Crittografia disco - Procedure Disaster Recovery

Controlli di accesso utente: viene stabilito un processo per assegnare account utente a persone autorizzate e per gestire efficacemente l'accesso minimo alle informazioni.

L’azienda ha individuato un processo per assegnare account utente a persone autorizzate e gestire efficacemente gli account in modo da fornire l'accesso minimo alle informazioni e limita l'accesso ai dati personali tenuti in determinati sistemi informativi.

Accesso ai dati

Nella “Struttura” sono attive le seguenti misure di sicurezza relative alla gestione dei dati da parte degli utenti, per contrastare le minacce e i possibili impatti delle schede “Accesso – accesso ai dati”.

Falsificazione identità, utilizzo non autorizzato	Sistema di autenticazione informatica - Sistema di procedure per la gestione delle credenziali - Sistema di Autorizzazione dei profili - Policy Password
Infiltrazione e manipolazione	Monitor network log - Cifratura traffico (https) - Firewall
Errori Utente	Formazione degli addetti

Sicurezza password di sistema

L’azienda ha individuato procedure di sicurezza password e "regole" per i sistemi informativi e possiede un sistema che rilevi qualsiasi accesso non autorizzato o uso anomalo. Le credenziali di accesso degli utenti (ad es. Un nome utente e una password o una *passphrase*) sono particolarmente sensibili e un attacco alle password tramite "forza bruta" è una minaccia comune.

Protezione da malware

L'azienda ha individuato efficaci difese anti-malware per proteggere i computer e garantisce che i dati personali siano protetti contro i malware. Giacché i computer possono essere infettati da malware (ad esempio virus, worm, trojan, spyware) tramite allegati di posta elettronica, siti web e supporti rimovibili che possono causare la perdita o compromettere i dati personali.

Backup e ripristino: stabilire un processo per eseguire regolarmente il backup delle informazioni elettroniche, per aiutare a ripristinare le informazioni in caso di disastro

L'azienda ha individuato un processo per eseguire regolarmente il backup delle informazioni elettroniche e aiutare, ripristinare le informazioni in caso di un incidente e garantisce la protezione contro la perdita di dati personali. Giacché è necessario eseguire backup periodici in modo da avere la possibilità di ripristinare i dati personali in caso di eventi imprevedibili o guasti a livello hardware, la frequenza dei backup (giornaliera) riflette la sensibilità e la riservatezza dei dati personali e la loro importanza per il continuo funzionamento del business.

Gestione delle patch

L'azienda ha individuato un processo per garantire che i software siano aggiornati e che siano applicati gli ultimi aggiornamento riguardanti la protezione dei dati, in modo da impedire lo sfruttamento delle vulnerabilità tecniche.

Firewall perimetrale

L'azienda ha individuato *firewall* per proteggere i computer da attacchi esterni e garantire la protezione dei dati personali in rete. Un firewall ben configurato è la prima linea di difesa contro attacchi esterni e aiuta a prevenire la violazione dei dati.

MISURE DI SICUREZZA ADOTTATE PER IL TRATTAMENTO DEI DATI SECONDO CLASSI DI RISCHIO

COMPORTAMENTI DEGLI OPERATORI

Sottrazione di credenziali di autenticazione:

Custode; Antifurto; Sbarre alle finestre; Allarme Vigilanza; Cancelli; Porte con serrature; Serrande

Carenza di consapevolezza, disattenzione o incuria:

Pianificazione backup; Procedure automatizzate; Formazione addetti backup; Formazione degli addetti

Comportamenti sleali fraudolenti:

Sistema di autenticazione informatica; Sistema di procedure per la gestione delle credenziali; Sistema di Autorizzazione dei profili; Policy Password

EVENTI RELATIVI AL CONTESTO

Sottrazione di strumenti contenenti dati

Uffici presidiati; armadi chiusi a chiave; cassettiera con serratura

Eventi distruttivi, naturali o artificiali

Gruppo i continuità; Messa a terra con revisione; Revisione periodica estintori; Addetti antincendio con corso

Guasto ai sistemi complementari

Contratto di assistenza; Impianto di condizionamento

Errori umani nella gestione della sicurezza fisica

Custode; Antifurto; Sbarre alle finestre; Allarme Vigilanza; Cancelli; Porte con serrature; Serrande

EVENTI RELATIVI AGLI STRUMENTI

Azione di virus informatici o di programmi

Antivirus; Antispam; Anti malware; OS Update; Crittografia disco; Procedure Disaster Recovery

Spamming o tecniche di sabotaggio

Configurazione firewall software; Configurazione antivirus; Configurazione antispam

Malfunzionamento, indisponibilità o degrado

Apparecchiature di scorta; Duplicazione componenti Hw

Accessi esterni non autorizzati

Sistema di autenticazione informatica; Sistema di procedure per la gestione delle credenziali; Sistema di Autorizzazione dei profili; Policy Password

Intercettazione di informazioni in rete

Monitor network log; Cifratura traffico (https); Firewall