sistemi SIROS

Allegato 1

SERVIZIO DI ADEGUAMENTO COMPLETO AL NUOVO REGOLAMENTO UE 679/2016

DESCRIZIONE DETTAGLIATA DELLE ATTIVITA'

SERVIZIO DI CONSULENZA

Il nostro metodo di lavoro prevede:

- Un'analisi delle caratteristiche e necessità della realtà atta a comprendere tutti gli aspetti legati alla gestione dei dati personali, al comportamento corrente sul trattamento dei dati, alla rete informatica ed alla gestione dei supporti cartacei.
- Una definizione degli interventi da adottare (a livello di procedure da intraprendere, di pianificazione di scadenze ed attività, di formazione del personale, di interventi su hardware e software, ecc.);
- Un'assistenza personalizzata in base alle esigenze del Cliente.

Per applicare i metodi di lavoro indicati, il nostro gruppo di esperti, altamente qualificati, è in grado di fornire ad Enti Pubblici ed Aziende Private un adeguamento completo.

Informazione dettagliata sul contenuto del nuovo Regolamento UE 679/2016
Riunione Iniziale

Effettuata presso l'Ente Titolare del Trattamento, alla presenza dei Responsabili del Trattamento, è finalizzata a illustrare gli adempimenti relativi al nuovo regolamento UE 679/2016 e quanto questa impone sulla metodologia di trattamento dei dati personali.

Mappatura dei processi

L'obiettivo è verificare l'effettiva organizzazione dell'Ente, rilevare tutti i settori interessati dal trattamento dei dati e mappare tutti i processi che interessano il singolo settore, predisporre un cronoprogramma per poter pianificare un piano di intervento che porti alla realizzazione di tutte le attività necessarie per l'adeguamento dell'Ente.

Identificazione dei dati personali trattati

Sarà verificato e aggiornato l'elenco dei dati personali previsto nel DPSS (Documento Programmatico Sulla Sicurezza). In caso di indisponibilità del DPSS, saranno predisposte delle schede questionario per inventariare i dati personali trattati, finalizzate al reperimento delle seguenti informazioni:

- Tipologia dei dati personali
- Numero delle banche dati in cui i dati personali sono conservati e localizzazione delle stesse
- Finalità del trattamento
- Incaricati al trattamento medesimo
- Modalità di custodia dei documenti cartacei

- Uffici in cui gli archivi cartacei sono collocati
- Incaricati che hanno accesso agli uffici e agli archivi

Necessaria, in tale fase, la diretta partecipazione dei responsabili di settore e degli incaricati del trattamento.

Censimento dei Trattamenti

Verrà effettuato il censimento dei dati personali presenti e dei relativi trattamenti, si dovrà riportare alle singole risorse l'incarico di trattare quel particolare dato.

Censimento e analisi dei sistemi applicativi software

Saranno censiti e analizzati gli applicativi software in dotazione dell'Ente a livello generale e per singola postazione di lavoro.

Analisi del rischio (PIA)

Sarà effettuata un'analisi dei rischi e verrà predisposto un piano di implementazione per la "Protezione dei Dati Personali".

I metodi per realizzare il PIA sono i medesimi dell'audit, rappresenta uno strumento più ufficiale e certificante, che viene sempre attuato da esterni all'organizzazione per valutare l'idoneità del sistema a determinate norme.

La nascita del sistema di protezione avviene contemporaneamente con l'evento di rischio di cui si deve fare trattamento e quindi non si fa trattamento fintantoché l'intero sistema non è stato definito **(Privacy by Design).**

L'articolo 25 (Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita) si esprime in tal senso:

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la ***pseudonimizzazione****, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.*

Il concetto di **Privacy by Default** esprime il fatto che si chiede di utilizzare il numero di informazioni necessario e sufficiente al trattamento in atto per limitare già in fase di progettazione il rischio privacy.

Vantaggi:

- Crea un sistema di preallarme, un modo per rilevare problemi di privacy costruendo garanzie in anticipo ed evitando problemi di investimento successivi;
- Evita errori costosi o imbarazzanti sulla privacy;
- Fornisce la prova che l'organizzazione ha tentato di evitare rischi per la privacy (ridurre la responsabilità, pubblicità negativa, danni alla reputazione);
- Migliora il processo decisionale;
- Dimostra a dipendenti, collaboratori, cittadini che l'organizzazione applica il processo di Privacy in misura adeguata e responsabile.

Aspetti economici e sinergie

Ogni attività che dovrà essere intrapresa per organizzare, monitorare e controllare gli aspetti legati al trattamento dei dati personali ha un preciso costo.

Un costo che cresce quanto più si trascurano gli aspetti preventivi legati alla mitigazione del rischio.

Gli articoli 83 (Condizioni generali per infliggere sanzioni amministrative pecuniarie) e 84 (Sanzioni) specificano i criteri da adottarsi per sanzionare l'attore inadempiente.

Sanzioni che non possono essere trascurate e che diventano elevate solo se non si è in grado di aver creato, mantenuto e gestito un Sistema Privacy di qualità.

Come in ogni sistema di qualità, diventano importanti le sinergie che si devono instaurare fra gli attori del processo privacy miranti ad un miglioramento continuo di ogni fase, ad una migliore distribuzione dell'informazione e della formazione.

Processo di Data Breach

Il processo di Data Breach gestisce i casi di "**violazione dei dati personali**", cioè qualsiasi *violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (art.4 paragrafo 12);*

Termine brevissimo per la comunicazione : **72 ore dalla scoperta**

Il mancato rispetto di questo obbligo comporta **sanzioni penali**.

Eccezione: non è obbligatorio se è improbabile che la violazione dei dati presenti un rischio per i diritti e le libertà delle persone.

Deve indicare almeno la natura della violazione, le categorie, il numero di interessati e di registrazioni coinvolti, le probabili conseguenze, le misure adottate o da adottare per porre rimedio alla violazione

Se la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà degli interessati è obbligatorio comunicare agli stessi la violazione senza giustificato ritardo, salvo che i dati fossero stati resi incomprensibili (ad es. cifratura), oppure siano adottate misure per scongiurare il rischio di lesione, ovvero la comunicazione richieda uno sforzo sproporzionato (in questo caso è necessaria una comunicazione pubblica o similare).

Identificazione dei ruoli

Saranno identificati i ruoli relativi ai Responsabili del trattamento dei dati personali, in generale, o i Responsabili/Incaricati specifici delle varie fasi di adeguamento (es: Responsabile e/o Incaricato della custodia delle credenziali di autenticazione, Responsabile e/o Incaricato delle copie di backup, etc.).

Verifica della strumentazione informatica

La verifica della strumentazione informatica è fondamentale prima di procedere all'applicazione concreta delle Misure minime di Sicurezza.

Gli articoli 22 e 32 del regolamento, fanno un esplicito riferimento alle misure di sicurezza informatiche.

Per mantenere la sicurezza e prevenire trattamenti in violazione al GDPR è necessario dunque:

- valutare attentamente il rischio informatico dell'organizzazione analizzando i seguenti aspetti:
  - danneggiamento di hardware e software;
  - errori nell'esecuzione delle operazioni nei sistemi;
  - malfunzionamento dei sistemi;
  - programmi indesiderati;
- attuare misure tecnologiche atte a garantire la limitazione dei rischi.
  Ad esempio:
  - cifratura dei dati;
  - livelli di resilienza dei sistemi;
  - disaster recovery;
- fare attenzione al perimetro di azione degli utenti nel sistema informativo. Infatti elemento comune e caratteristico degli attacchi più pericolosi è l'assunzione del controllo remoto della macchina attraverso una scalata ai privilegi;
- dotarsi di efficaci strumenti di rilevazione, in grado di abbreviare i tempi, oggi pericolosamente lunghi, che intercorrono dal momento in cui l'attacco primario è avvenuto e quello in cui le conseguenze vengono scoperte.

Verifica Applicazione Misure Minime Postazione

Una volta definite credenziali e sistema di autenticazione sul server si deve procedere alla definizione di codici di accesso sulle singole postazioni volti ad evitare trattamenti non consentiti ed illeciti ed alla verifica sulle medesime postazioni degli strumenti necessari alla protezione dei dati.

REDAZIONE DEI DOCUMENTI

Redazione Registro del Titolare del trattamento
Redazione Registro del Responsabile del trattamento

I registri da conservare e mantenere sono due e la conservazione può avvenire in forma cartacea ma anche in forma elettronica, rendendo sempre disponibile il dato ad eventuali ispezioni dell'autorità garante.

Il registro del **titolare del trattamento**, contiene:

- Anagrafica del titolare stesso, di un contitolare se presente, del rappresentante e del titolare alla protezione dati;
- Le finalità del trattamento;
- Le categorie degli interessati a cui fa capo il dato;
- Eventuali termini per la cancellazione automatica del dato;
- Un'eventuale descrizione generale delle misure di sicurezza tecnico-organizzative.

Il registro del **responsabile del trattamento**, in cui sono presenti:

- L'anagrafica dei responsabili del trattamento;

- La descrizione delle categorie di trattamento effettuati;
- Opzionalmente la descrizione delle misure di sicurezza intraprese.

Redazione PIA (Privacy Impact Assessment)

Sarà redatto un piano che valuta la rischiosità complessiva per ogni fenomeno, azioni intraprese e rischiosità residua ed un piano di azione in cui viene definito in quale modo verrà mitigato il singolo rischio, coloro che sono incaricati di operare in tal senso e l'eventuale costo previsto per l'attività.

Redazione Lettere di incarico a Responsabili/ Incaricati del trattamento

Il nuovo Regolamento UE impone al Titolare del trattamento di redigere per iscritto le lettere di nomina dei Responsabili/Incaricati al trattamento.

Redazione Modello comunicazione Data Breach

Il nuovo Regolamento UE impone al Titolare/Responsabile del trattamento di comunicare per iscritto la violazione dei dati.

Redazione Modello comunicazioni agli organi di controllo

Verranno redatte tutte le comunicazioni agli Organi di Controllo, comprese eventuali modelli di comunicazione che dovessero insorgere nel futuro.

Redazione Modello Informative e consenso

Saranno predisposti i documenti relativi alle informative e consenso.
Il regolamento europeo si esprime definendo **consenso dell'interessato** *qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.*
Quindi, in ogni caso, l'interessato dovrà esprimersi in merito al trattamento fornendo un consenso effettivo ed inequivocabile, ad esempio, con dichiarazione scritta o attraverso mezzi elettronici o verbale (con registrazione).
Dovranno sparire le formule per cui la mancanza di opposizione ad un trattamento diventa implicitamente un assenso. **Sparisce di fatto il consenso assenso.**
L'interessato ha il diritto di revocare qualsiasi consenso abbia dato e deve essere informato di questo dal titolare del trattamento. Restano leciti tutti i trattamenti compiuti prima della revoca stessa.

Rilascio e personalizzazione di tutti i modelli necessari agli adempimenti privacy

Saranno predisposti e personalizzati tutti i modelli necessari per gli adempimenti al Nuovo Regolamento Europeo 2016/679 sulla privacy.

Supporto per la predisposizione della Delibera di affidamento

Per gli Enti Locali la Siros Sistemi. fornisce un servizio di supporto informativo per la predisposizione dell'atto di natura regolamentare per un eventuale affidamento a terzi.

FORMAZIONE DEL PERSONALE

Formazione del personale

L'art. 32 del regolamento, al paragrafo 4 cita esplicitamente il ruolo centrale della formazione per chiunque abbia accesso al trattamento dei dati:

"il titolare del trattamento ed il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri".

Ogni Ente pertanto dovrà:

- pianificare un percorso ed un piano di formazione;
- integrare la formazione con le tematiche relative alla digitalizzazione dei processi, la riforma del Codice di Amministrazione digitale, i codici di comportamento degli enti e con le ultime recenti novità normative in materia di trasparenza, prevenzione della corruzione, FOIA e whistleblowing.
- pubblicare i materiali formativi nella sezione intranet dell'organizzazione al fine di costituire un presidio di informazione e aggiornamento a beneficio di tutti e di inserire i sopra citati atti come allegati al registro del trattamento.

La formazione verrà erogata presso la sede del vostro Ente.