Modello Organizzativo Privacy& Security

ACSAL ASSOCIAZIONE CULTURA E SVILUPPO ALESSANDRIA

PIAZZA FABRIZIO DE ANDRÉ, 76 - 15121 ALESSANDRIA

CODICE FISCALE E PARTITA IVA: 01734560061

Aggiornamento del 08.01.2024

CONTENUTI DEL DOCUMENTO

1. SCOPO DEL MODELLO ORGANIZZATIVO PRIVACY & SECURITY

Scopo del presente Documento è quello di descrivere e documentare le politica, la struttura organizzativa, le responsabilità e tutte le attività che regolamentano l'istituzione, la gestione ed il funzionamento del Modello organizzativo di protezione dei dati personali ai sensi del Regolamento UE 2016/679, che è finalizzato ad individuare i principali eventi potenzialmente dannosi per la sicurezza dei dati, valutarne le possibili conseguenze e la gravita e porli in correlazione con le idonee misure da adottare.

La corretta gestione dei dati personali viene, con la nuova normativa di riferimento, considerata fondamentale per garantire la riservatezza di coloro cui appartengono i dati trattati: pertanto la sicurezza delle informazioni non è più un fatto esclusivamente legato alla difesa del patrimonio conoscitivo del Soggetto Giuridico.

In questo scenario, la valutazione dell'adeguatezza delle misure di sicurezza adottate è fondamentale per garantire la conformità alla normativa, ma soprattutto la tutela dei diritti dell'interessato.

Il Regolamento UE 2016/679 non individua le misure da adottare in caso di trattamento dei dati con o senza strumenti elettronici ma demanda al Titolare del trattamento il compito di definirle in relazione all'analisi dei rischi effettuati.

Il Titolare e i Responsabili hanno l'obbligo di adottare delle misure tecnico-informatiche, organizzative e logico-procedurale, in grado di rispettare quanto previsto dalla normativa.

Le misure devono garantire che i dati siano riservati, vale a dire che si mettano in atto tutte le forme di prevenzione per scongiurare i rischi di utilizzi indebiti di informazioni. In pratica i dati devono essere accessibili solo alle persone autorizzate, pertanto è necessaria un'ottima conoscenza del flusso dei dati dall'interno all'esterno dell'attività.

Tra le misure individuate, è presente la stessa Analisi dei Rischi, che ha lo scopo di individuare i principali eventi potenzialmente dannosi per la sicurezza dei dati, valutarne le conseguenze e la gravità e porli in correlazione con le misure previste.

Il giudizio di adeguatezza, come indicato dal Regolamento UE 2016/679, deve essere parametrizzato in base ai seguenti criteri:

- le conoscenze acquisite in base al processo tecnico;
- la natura dei dati;
- le specifiche caratteristiche del trattamento.

La tutela dei dati è il frutto di un'attività composita e permanente: non esiste una sicurezza assoluta ma una tendenza ottimale verso la minimizzazione del rischio in considerazione della tutela dei diritti. Essa richiede interventi di tipo organizzativo, fisico e logico sottoposti a continuo aggiornamento e verifica. Il tutto condito con un adeguato programma di informazione e sensibilizzazione ai diversi livelli dei responsabili dei dati e degli eventuali servizi esterni.

I dati personali devono essere protetti senza considerare la loro forma o il supporto (cartaceo, informatico o di altro tipo) su cui sono registrati. Si ricorda, infatti, che entrano nella definizione di dato personale anche immagini quando idonei ad individuare un soggetto.

Le misure minime di sicurezza devono essere adottate da tutti coloro che, per le attività svolte rientrano nell'ambito applicativo della normativa in materia di dati personali; quindi non solo dall'Organizzazione, ma anche da quei terzi che utilizzano tali dati per conto dell'Organizzazione.

2. PRINCIPI CHE DETERMINANO IL TRATTAMENTO DEI DATI

I dati personali devono essere trattati secondo principi espressi dal legislatore comunitario nell'art. 5 del Regolamento UE 679/2016 di seguito riportati:

PRINCIPIO DI LICEITÀ, CORRETTEZZA E TRASPARENZA: i dati devono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.

PRINCIPIO DI GESTIONE PER FINALITÀ: i dati devono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità.

PRINCIPIO DI MINIMIZZAZIONE: i dati devono essere trattati in modo adeguato, pertinente e limitato a quanto necessario rispetto alle finalità per le quali sono trattati.

PRINCIPIO DI ESATTEZZA: i dati devono essere 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.

PRINCIPIO DI LIMITAZIONE DELLA CONSERVAZIONE: i dati devono essere 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

PRINCIO DI INTEGRITÀ E RISERVATEZZA: i dati devono essere trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

3. CONDIZIONI PER IL CONSENSO ED INFORMATIVA

Come riportato dall'art. 6 del Regolamento UE 679/2016, il Titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.

La richiesta di consenso deve essere presenta in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro.

Prima di esprimere il proprio consenso, l'interessato è informato delle modalità di gestione del trattamento dei dati tramite apposita informativa, conforme agli art. 13 e 14 del Regolamento UE 679/2016, che deve riportare le seguenti informazioni:

- identità del Titolare e del Responsabile del trattamento
- finalità e destinatari del trattamento
- periodo di conservazione dei dati
- diritti dell'interessato

Si riportano in allegato 1 "Linee Guida Gestione Consensi", documento utile per la redazione di informative e consensi.

4. TERMINI SPECIFICI USATI DAL LEGISLATORE

TERMINE	DEFINIZIONE come riportato dall'art. 4 del Regolamento UE 679/2016
Trattamento:	qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione
Dato personale:	qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
Dati relativi alla salute:	i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute
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
Titolare del trattamento:	la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri
Responsabile del trattamento:	la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
Violazione dei dati personali:	la 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;
Profilazione:	qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica
Pseudonimizzazione:	il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile

5. STRUTTURA DEL MODELLO ORGANIZZATIVO

Ai fini della redazione del presente Documento si è operato secondo le fasi di analisi di seguito.

5.1 IDENTIFICAZIONE DELLA STRUTTURA

Si è provveduto all'identificazione e definizione dei compiti e delle responsabilità nell'ambito delle Strutture preposte al trattamento dei dati, con riferimento agli art. 27 e 28 del Regolamento UE 679/2016.
I risultati dell'analisi sono riportati nell'allegato 2 "Organigramma Privacy".

5.2 IDENTIFICAZIONE DEI REGISTRI DI TRATTAMENTO

Si è provveduto a redigere il registro dei trattamenti, definendo le modalità di gestione di tali registri in accordo all'art. 30 del Regolamento UE 679/2016.
I registri di trattamento sono riportati in allegato 3 "Registri trattamento dati".

5.3 ANALISI DEI RISCHI

Per la gestione delle analisi dei rischi, con riferimento all'art. 30 del Regolamento UE 679/2016, si è partiti dalla considerazione che le risorse coinvolte nel trattamento sono di tre categorie, come di seguito riportato.

TERMINE	DEFINIZIONE
Sicurezza logica	Il campo di applicazione della sicurezza logica riguarda principalmente la protezione dell'informazione, e di conseguenza di dati, sia in relazione al loro corretto funzionamento ed utilizzo, sia in relazione alla loro gestione e manutenzione nel tempo. Le contromisure di sicurezza logica sono da intendersi come l'insieme di misure di carattere tecnologico che concorrono nella realizzazione del livello di sicurezza da raggiungere. È importante che siano sempre disponibili e funzionanti i prodotti software posti a presidio della sicurezza dei dati trattati e che sia garantita la puntualità dei salvataggi per la continuità del servizio. Inoltre, per garantire la riservatezza delle informazioni, l'accesso ai dati non deve essere consentito a persone non autorizzate e i dati devono essere resi disponibili solo a chi ha necessità di utilizzarli per svolgere le proprie funzioni
Sicurezza fisica	Sono le funzioni di sicurezza che il sistema dovrà garantire a tutti i livelli di elaborazione. Sono individuati i seguenti servizi di sicurezza atti a verificare e confermare che l'identità dichiarata di un utilizzatore sia autentica ed a garantire che i dati personali siano fisicamente protetti dall'accesso non autorizzato da parte di terzi che non siano soggetti autorizzati al trattamento
Sicurezza organizzativa	Accanto all'adozione di misure tecnologiche, è necessario che vengano definite una serie di norme e procedure miranti a regolamentare gli aspetti organizzativi del processo di sicurezza e le regole comportamentali per i soggetti autorizzati al trattamento, con la definizione di ruoli, compiti e responsabilità per la questione di tutte le fasi de processo di sicurezza

L'analisi dei rischi è riportata nell'allegato 4 "Analisi dei rischi".

6. TRATTAMENTI AFFIDATI ALL'ESTERNO

Per quanto attiene ai trattamenti affidati all'esterno sono stati identificati e specificati i soggetti terzi ai quali sono affidati i dati personali ed i relativi trattamenti, direttamente all'interno dei registri di trattamento.
I soggetti terzi a cui sono affidati trattamenti dati in Out-Sourcing sono selezionati il base a requisiti di esperienza, capacità ed affidabilità tali da fornire idonea garanzia del pieno rispetto delle disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza). La nomina di responsabile esterno al trattamento è appositamente formalizzata (allegato fac simile "Nomina responsabile esterno al trattamento").

7. INTERVENTI FORMATIVI ED INFORMATIVI

In considerazione dell'importanza da attribuire alla consapevolezza ed al comportamento di tutto il personale (dipendenti e collaboratori stabili) addetto al trattamento dei dati personali, il Modello Organizzativo prevede gli interventi informativi/formativi di seguito specificati ed indicati nell'allegato 5 "Procedura Formazione":

- distribuzione a tutto il personale addetto al trattamento dei dati personali di apposita procedura di gestione della privacy e delle relative istruzioni di gestione dei dati (allegato 6 "Procedura gestione privacy")
- momenti di sensibilizzazione in termini di conoscenza della normativa, analisi e spiegazione dei ruoli misure minime ed appropriate di sicurezza
- momenti informativi/formativi in caso di ingresso in servizio di nuovo personale; cambiamento di mansioni, definizione di nuove misure di sicurezza, emanazione di nuove disposizioni legislative in materia di tutela dei dati personali.

8. PIANO DI VERIFICA DELLE MISURE ADOTTATE

Il Modello Organizzativo prevede la presenza di momenti di audit, un processo sistematico ed indipendente finalizzato a stabilire se quanto pianificato a livello organizzativo generale o più in dettaglio a livello comportamentale:

- è coerente con i requisiti del Regolamento UE 679/2016
- è coerente con quanto stabilito nell'analisi dei rischi in tema di misure di sicurezza
- risulta efficace, cioè adeguato al conseguimento degli obiettivi pianificati in termini di tutela dei dati trattati.

Tali audit, descritti nella procedura "Gestione audit" (allegato 7) consentono di individuare eventuali azioni di miglioramento, atte ad aumentare il livello di sicurezza dei dati implementato con il presente Modello Organizzativo.

9. PROCEDURA DI NOTIFICA DI VIOLAZIONE DEI DATI PERSONALI

Il Modello Organizzativo prevede la presenza di una apposita "Procedura di notifica di violazione dei dati personali" (allegato 8), da utilizzare in caso di "Data Breach", cioè di una situazione che abbia provocato una violazione della sicurezza dei dati, e che quindi determini, accidentalmente o in modo illecito la distruzione, perdita, modifica, divulgazione, accesso, copia o consultazione non autorizzate di dati personali trasmessi, conservati o comunque trattati.

10 GESTIONE DELLE SEGNALAZIONI

Il Modello Organizzativo prevede la presenza di una apposita "Procedura gestione segnalazioni" (allegato 9) che formalizza le modalità attuate per la gestione delle richieste, delle segnalazioni e dei reclami in materia di trattamento dei dati personali, secondo quanto previsto dal Regolamento (UE) 2016/679: tale procedura si applica sia alle richieste da parte degli interessati che a quelle provenienti dal Garante per la Privacy.

11 GESTIONE DELLE INFORMAZIONI RISERVATE

Tutti i soggetti che operano e collaborano con ACSAL ASSOCIAZIONE CULTURA E SVILUPPO ALESSANDRIA sono tenuti a osservare le leggi in materia di abuso di informazioni riservate (insider trading).

Gli amministratori, i dipendenti ed i collaboratori e coloro che, a qualsiasi titolo, operino in nome e per conto di ACSAL ASSOCIAZIONE CULTURA E SVILUPPO ALESSANDRIA non possono utilizzare informazioni non di dominio pubblico acquisite in funzione della loro posizione all'interno dell'associazione.

Le informazioni, le conoscenze e le competenze tecniche sviluppate e gestite da ACSAL ASSOCIAZIONE CULTURA E SVILUPPO ALESSANDRIA costituiscono una risorsa importante che ciascuno deve tutelare, così da evitare un danno sia patrimoniale sia di immagine, rispettando quanto definito nella "Procedura gestione informazioni riservate" (allegato 10)

Di conseguenza, gli amministratori, i dipendenti ed i collaboratori e coloro che a qualsiasi titolo operino per conto di ACSAL ASSOCIAZIONE CULTURA E SVILUPPO ALESSANDRIA sono tenuti a non rivelare a terzi informazioni riguardanti le conoscenze tecniche, tecnologiche e commerciali di MI&T SRL, se non nei casi in cui tali informazioni siano richieste da leggi o da altre disposizioni regolamentari o laddove sia espressamente prevista da specifici accordi contrattuali.

Gli obblighi di confidenzialità i permangono anche dopo la cessazione del rapporto di lavoro o di collaborazione con ACSAL ASSOCIAZIONE CULTURA E SVILUPPO ALESSANDRIA.

12. ALLEGATI

Allegato 1: Linee Guida Gestione Consensi

Allegato 2: Organigramma Privacy

Allegato 3: Registro Trattamento Dati

Allegato 4: Analisi dei Rischi

Allegato 5: Procedura formazione

Allegato 6: Procedura Gestione Privacy

Allegato 7: Procedura Gestione Audit

Allegato 8: Procedura di Notifica di Violazione dei Dati Personali

Allegato 9: Procedura Gestione Segnalazioni

Allegato 10: Procedura gestione informazioni riservate