AGENZIA FORMATIVA
della PROVINCIA di VARESE

Modello Organizzativo e Disposizioni Operative per l'impostazione del sistema di gestione della Sicurezza delle Informazioni

(adeguamento al GDPR - Reg. UE 2016/679 - standard internazionali ISO 27001 e 27002)

Approvato con delibera del Consiglio di Amministrazione n° 3 del 28/01/2020.
Modificato con delibera del Consiglio di Amministrazione n° 12 del 23/03/2021.

Indice

SEZIONE 1 – PARTE GENERALE

Art. 1 - Premessa

Il regolamento europeo Reg. 2016/679 ("GDPR" – General Data Protection regulation) è immediatamente esecutivo.
Il presente documento serve a individuare con precisione le modalità, le prassi, la metodologia, le tecniche e gli strumenti mediante le quali, nell'ambito specifico dell'Agenzia, si raggiunge e si mantiene nel tempo l'adeguamento e la conformità alle prescrizioni del GDPR e si imposta un SGSI – Sistema per la Gestione della Sicurezza delle Informazioni e si possa dimostrare, in caso di controlli o ispezioni da parte degli organismi preposti, che l'Agenzia è in regola con le prescrizioni del succitato Regolamento UE 2016/679.

Art. 2 - Obiettivo del presente Regolamento

Il presente regolamento permette di raggiungere i seguenti obiettivi:

- implementare il principio fondamentale di responsabilizzazione ("accountability") introdotto dal GDPR, in base al quale il titolare deve non solo essere conforme alle prescrizioni del GDPR, ma deve anche essere in grado di dimostrare la conformità raggiunta;
- indicare metodologie e prassi operative specifiche per l'adeguamento alle prescrizioni del GDPR, tenendo conto del contesto specifico dell'Agenzia;
- in particolare, per quanto riguarda la sicurezza (art. 32), individuare precisamente una procedura per testare, verificare periodicamente e valutare regolarmente l'efficacia delle misure tecniche ed organizzative da mettere in atto per assicurare un adeguato livello di sicurezza e di protezione dei dati
- impostare un SGSI – Sistema di Gestione della Sicurezza delle Informazioni che permetta di dimostrare che l'Agenzia è conforme ai requisiti di sicurezza previsti dall'art. 32 del GDPR e conforme a riconosciuti standard di sicurezza a livello internazionale.

Art. 3 - Liceità dei trattamenti

Per ciascun trattamento effettuato, deve essere verificata e documentata per iscritto la liceità del trattamento stesso, individuata nella base giuridica che giustifica/richiede il trattamento specifico.
La base giuridica deve essere costituita da:

- funzioni istituzionali dell'Agenzia,
- norme di legge di rango primario.

Si dovrà inoltre verificare che non sussistano norme di legge che vietino esplicitamente il trattamento.

Art. 4 - Informativa agli interessati

Il GDPR prevede che, oltre a quanto già previsto dall'art. 13 del D.Lgs. 196/2003, l'informativa contenga le seguenti informazioni:

- i dati di contatto del responsabile della protezione dei dati
- la base giuridica del trattamento
- il tempo di conservazione dei dati personali o, se non è possibile, i criteri utilizzati per determinare tale periodo
- gli ulteriori diritti dell'interessato introdotti dal GDPR.

Art. 5 - Incaricati del trattamento dei dati

Il GDPR all'art. 29 - (Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento) specifica che "il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso ai dati personali, non può trattare 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. L'Agenzia, per chiarezza continuerà ad usare la dicitura "Incaricato del trattamento dei dati", intendendo con tale locuzione i soggetti di cui all'art. 29 del GDPR.

Art. 6 - Non applicabilità del requisito della portabilità dei dati

Sebbene l'art. 20 del GDPR preveda astrattamente il diritto dal parte dell'interessato alla portabilità dei dati, l'Agenzia non è tenuta a soddisfare le richieste di portabilità dei dati nei seguenti casi:

- nel caso di dati in formato cartaceo
- nel caso di trattamenti che prescindono dal consenso
- nel caso di dati forniti dall'interessato stesso.

Art. 7 - Tempi di conservazione dei dati e regole di scarto

Si applicano, per quanto compatibili alla natura dell'agenzia, le prescrizioni previste dalle normative di riferimento e le prescrizioni emesse dalla articolazione regionale di riferimento della Soprintendenza Archivistica a cui si possono affiancare eventuali prescrizioni definite internamente.

Art. 8 - Responsabili del trattamento

L'art. 28 del GDPR prevede una figura di "responsabile del trattamento" che può essere ricoperta solo da soggetti esterni. E' possibile designare in qualità di Responsabile esterno del trattamento dei dati il soggetto esterno all'Agenzia coinvolto a vario titolo nelle varie operazioni di trattamento dei dati, come ad esempio ditte incaricate dei servizi di assistenza e manutenzione degli apparati hardware oppure delle piattaforme software, con particolare riferimento alle piattaforme in cloud (es. registro elettronico, protocollo informatico in cloud, etc.).

SEZIONE 2 – SICUREZZA

Art. 9 - Obbligo di notificazione immediata di una violazione dei dati al Responsabile della protezione dei dati

Nel caso si verifichi un qualsiasi tipo di violazione dei dati, o se ne abbia anche solamente il sospetto, ne deve essere data immediata comunicazione al Direttore Generale e al Responsabile della protezione dei dati, il quale si attiverà immediatamente per valutare se vi sia stata effettivamente una violazione, la portata e le conseguenze, e valutare se sussistano i presupposti per effettuare la notificazione entro 72 ore all'autorità di controllo.

Art. 10 - Registro delle violazioni dei dati

Deve essere in ogni caso tenuto un registro di tutte le violazioni di dati verificatesi.
Il suddetto registro deve contenere almeno le seguenti informazioni:

- data della violazione
- descrizione delle circostanze e dell'evento
- tipologia e quantità di interessati impattati
- conseguenze della violazione
- data di comunicazione della violazione al Garante per la protezione dei dati (se la comunicazione è stata effettuata).

Art. 11 - Il modello MMS – Modello per il Monitoraggio della Sicurezza

La tracciatura degli eventi che possono accadere compromettendo la sicurezza, si effettua compilando il Modello MMS – Modello per il Monitoraggio della Sicurezza, qualora vi siano accadimenti il modello compilato deve essere inviato al Responsabile della protezione dei dati designato ai sensi dell'art. 37 del GDPR, alla mail rpd@agenziaformativa.va.it

Art. 12 - Effettuazione periodica di scansioni di vulnerabilità sulle piattaforme in cloud

E importante che vengano effettuate periodicamente delle scansioni di vulnerabilità delle piattaforme in cloud in uso all'agenzia per individuare e documentare debolezze e configurazioni poco sicure e per svolgere le attività di remediation.
Le scansioni di vulnerabilità verranno effettuate a cura del Responsabile della protezione dei dati.
Le scansioni saranno primariamente effettuate sulle piattaforme di più comune utilizzo (es. Sito web istituzionale).
A fronte di richiesta da parte del Direttore Generale, potranno venire effettuate una-tantum delle scansioni di vulnerabilità su altri oggetti esposti direttamente su internet e

dotati di indirizzo ip pubblico, come ad esempio firewall, router, server di posta elettronica etc.

Art. 13 - Il modello DMS – Documento sul Monitoraggio della Sicurezza

Gli eventi di cui all'articolo 12 devono essere oggetto di analisi periodica all'interno di un documento denominato DMS – Documento per il Monitoraggio della Sicurezza, predisposto dal Responsabile della protezione dei dati e posto all'attenzione del Direttore Generale e del Comitato per la Sicurezza e la Privacy. All'interno del DMS devono inoltre trovare trattazione esaustiva ed organica tutte le problematiche relative alla sicurezza e alla protezione dei dati personali che si sono verificate nel trimestre di riferimento, come ad esempio:

- l'esternalizzazione di un nuovo trattamento di dati
- la predisposizione di una procedura operativa o di un regolamento ad-hoc
- la predisposizione di una lettera di nomina
- la predisposizione di una nuova informativa
- la predisposizione di comunicazioni ai dipendenti o agli interessati
- il recepimento di norme o linee guida emesse a livello nazionale od europeo, concernenti la sicurezza o la protezione dei dati
- l'analisi di una richiesta di accesso ai dati
- la revisione dei Registri del trattamenti dei dati
- lo svolgimento di un DPIA – Data Protection Impact Assessment
- la verifica del soddisfacimento dei principi di Privacy by Design e Privacy by default all'interno di un sistema o di un processo

Art. 14 - Requisiti per il raggiungimento di un adeguato livello di sicurezza nei trattamenti effettuati

Dovranno comunque essere messe in atto le misure minime di sicurezza previste dagli artt. 33, 34 e 35 del D.Lgs. 196/2003, nei modi previsti dal Disciplinare Tecnico (Allegato B al D.Lgs. 196/2003), nonché le misure minime di sicurezza previste dalla Circolare AGID 2/2017.

Art. 15 - Il Comitato SP – Comitato per la Sicurezza e la Privacy

Per assicurare un adeguato livello di attenzione e di potere decisionale in merito a tutte le questioni riguardanti la sicurezza e la protezione dei dati personali, potrà essere costituito un Comitato per la Sicurezza e la Privacy (per brevità denominato "Comitato SP"), composto dai seguenti membri permanenti:

- Direttore Generale
- Responsabile della protezione dei dati.
- Un Responsabile di sede individuato dal Direttore

Il suddetto Comitato analizzerà periodicamente tutte le problematiche inerenti la sicurezza e la privacy che si sono verificate e analizzare tutti i modelli MMS e DMS prodotti.

Art. 16 - Dimostrazione della conformità ai requisiti di sicurezza previsti dall'art. 32 del GDPR

In caso di verifiche da parte del Garante per la protezione dei dati o della Guardia di Finanza o delle autorità preposte, l'Agenzia deve dimostrare che ha messo in atto un sistema di gestione della sicurezza tale da soddisfare i requisiti previsti dall'art. 32 del GDPR.
A tal fine l'adesione a codici di condotta approvati o ad uno schema di certificazione può essere addotto come elemento per comprovare la conformità ed un adeguato livello di sicurezza e di protezione dei dati.

Art. 17 - Gestione della sicurezza secondo codici di comportamento o meccanismi di certificazione

L'Agenzia ha facoltà di ricorrere a codici di condotta e a schemi di certificazione per dimostrare la conformità ai requisiti di cui all'art. 32 comma 1 del GDPR.
Allorquando i suddetti codici di condotta e/o schemi di certificazione siano stati emessi dal Garante per la protezione dei dati personali ed approvati rispettivamente ai sensi degli artt. 40 e 42 del GDPR, viene data facoltà all'Agenzia di aderire ai suddetti codici e schemi, con il coordinamento e la consulenza del Responsabile della protezione dei dati.
Nel caso in cui entro la data di ultimo aggiornamento del presente documento i suddetti codici di condotta e/o meccanismi di certificazione approvati non siano stati ancora emessi dall'Autorità Garante per la protezione dei dati personali, viene data facoltà al Responsabile della protezione dei dati di valutare, proporre e coordinare l'adesione a schemi internazionali di certificazione di sicurezza, al fine di poter dimostrare la conformità ai requisiti dell'art. 32 del GDPR – Sicurezza del trattamento, secondo il principio di responsabilizzazione ("accountability"), e di mettere in atto un SGSI – Sistema per la Gestione della Sicurezza delle Informazioni conforme (ad esempio) ai seguenti standard internazionali di sicurezza:

- ISO / IEC 27001 (norma vera e propria)
- ISO / IEC 27002 (best practice e raccomandazioni in materia di sicurezza)
- Annex-A ("Control Objectives and Controls").