ANNESSO A9
Policy per la riservatezza dei dati e dei documenti gestiti nel sistema di protocollo informatico

LEGENDA

Dato personale, ex art. 4, comma I, nr. 1, Reg. 679/2016, General Data Protection Regulation (GDPR)
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;

Categoria particolare di dati personali, ex art. 9, nr. 1, GDPR
Dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Dati personali relativi a condanne penali e reati, ex art. 10, nr. 1, GDPR
Dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Sistemi IT
Ogni sistema informatico o comunque ogni applicativo o portale, proprietario o in licenza di cui è titolare o licenziatario Avepa o che quest'ultima legittimamente utilizza.

LA SICUREZZA DEI DATI

I dati personali, siano essi in formato digitale oppure su supporto cartaceo, devono essere custoditi con cura al fine di preservarne le caratteristiche di integrità, disponibilità e confidenzialità.
Il Considerando n. 39 del GDPR specifica che: "I dati personali dovrebbero essere trattati in modo da garantirne un'adeguata sicurezza e riservatezza, anche per impedire l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento".
Il principio della "responsabilizzazione" ("accountability") impone di mettere in atto "misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al regolamento".
In ragione del fatto che i trattamenti possono essere effettuati con o senza l'ausilio di strumenti elettronici, le misure di sicurezza da adottare devono essere differenti ed adeguate alle diverse situazioni ed alla natura dei dati trattati.
La valutazione del livello di sicurezza e dei rischi collegati per l'adempimento di cui all'art. 32 viene integrata dall'implementazione della norma ISO 27001, e della relativa certificazione, e dello standard ISO 29151.

A seguito del mutato quadro normativo europeo in materia di privacy, l'AVEPA ha provveduto con decreto del Direttore n. 87/2018 del 25/05/2018 ad una ridefinizione delle misure organizzative e tecniche per assicurare il rispetto del nuovo regolamento (UE) 2016/679, nonché a fornire nuove istruzioni per il trattamento di dati personali, approvando inoltre i seguenti documenti:

- Misure Organizzative e tecniche per il trattamento dei dati personali;
- Privacy Policy ed Istruzioni operative G1;

- registro del trattamento costituito dal modello di Risk Matrix e dal registro del trattamento dei Responsabili esterni.

Trattamenti effettuati con l'ausilio di strumenti elettronici
Nel caso di trattamenti di dati personali effettuati con strumenti elettronici, sono adottate le misure tecniche di seguito indicate:

a) il trattamento di dati personali con strumenti elettronici è consentito solo alle "persone autorizzate", dotate di credenziali di autenticazione univoche. Le predette credenziali di autenticazione non possono essere assegnate ad altre persone, neppure in tempi diversi.
b) l'amministrazione individua l'ambito del trattamento consentito alle singole persone autorizzate attraverso l'attribuzione del "profilo di autorizzazione" adeguato all'ambito di trattamento consentito. Deve inoltre verificare periodicamente la sussistenza delle condizioni per la conservazione del profilo di autorizzazione assegnato alla persona autorizzata. I "profili di autorizzazione" sono l'insieme delle facoltà operative/operazioni, tecnicamente consentite dal sistema informatico/applicativo, in relazione all'ambito di trattamento consentito al medesimo.
c) i documenti che contengono dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, o che contengano dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (art. 9 GDPR), vengono gestiti, nel momento della registrazione in Docway, con l'attribuzione del livello di visibilità "confidenziale". Tale attributo della registrazione consente la visibilità del contenuto della stessa ai soli soggetti cui è stata assegnata in competenza o in conoscenza.
d) i documenti che contengono dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, vengono gestiti, secondo le policy di riservatezza dell'ente, con l'assegnazione alle sole persone incaricate del trattamento per il quale i documenti sono stati acquisiti.

Trattamenti effettuati senza l'ausilio di strumenti elettronici
Nel caso di trattamenti effettuati senza l'ausilio di strumenti elettronici, sono adottate le misure tecniche di seguito indicate, anche nell'ipotesi di copie/riproduzioni degli atti originali:

a) i documenti che contengono dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, o che contengano dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (art. 9 GDPR) sono conservati in busta chiusa all'interno dei fascicoli cartacei cui appartengono;
b) i documenti che contengono dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, o che contengano dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (art. 9 GDPR) devono essere spostati da una struttura all'altra solo quando sia strettamente necessario. Se trasportati:
    - ✓ devono essere inseriti in una busta chiusa e sigillata (es. firma sulla chiusura che ne renda evidente l'eventuale violazione);
    - ✓ devono essere protetti (imbustati) da colui che lo detiene per competenza, non affidati ad altro soggetto affinché vi provveda;
    - ✓ la busta chiusa che li contiene deve recare solamente il nome del mittente e del destinatario, senza alcun riferimento, seppur generico, al contenuto della stessa.

POLITICHE RELATIVE ALLA RIDUZIONE DEL RISCHIO PRIVACY (GDPR)

L'Agenzia ha adottato apposite policy a completare, per una maggiore sicurezza della gestione delle informazioni in ottica privacy, quanto già viene attuato mediante i controlli della norma ISO27001:2013. Il focus viene effettuato basandosi sul GDPR e sulle linee guida del Garante, seguendo lo standard ISO29151.

29151-A.5 Limitazione della raccolta dei dati

Limitare la raccolta dei dati a quanto richiesto e a quanto serve per gli scopi specifici previsti da regolamenti, normative, decreti ministeriali e circolari specifiche (es. Agea).

29151-A.6 – Minimizzazione dei dati: i dati devono essere adeguati, pertinenti e limitati alla finalità per cui sono raccolti.

Nella definizione di nuove procedure, una specifica fase dell'analisi è dedicata all'individuazione del dataset da utilizzare, allo scopo di renderlo funzionale allo scopo e non eccessivo, pertinente e limitato alle finalità dell'applicazione, tenendo conto della Normativa Comunitaria, della Normativa Nazionale e Regionale, nonché di eventuali richieste da parte di Agea, del MIPAAF, del MEF, e di organismi certificatori autorizzati.
Nel caso di utilizzo di dati a fini statistici viene considerato il minimo dataset possibile per l'esecuzione dell'analisi statistica stessa. Se possibile, e coerentemente con l'informativa, i dati vanno anonimizzati, altrimenti comunque si considererà il minimo dataset possibile per raggiungere lo scopo.
I dati vengono utilizzati limitatamente allo scopo per cui sono raccolti, con particolare riferimento all'informativa che ne declina gli scopi.

29151-A.7.2 – Cancellazione sicura

Il responsabile della trasparenza adotta una procedura per la gestione della cancellazione dei dati esposti al pubblico, una volta scaduti i termini di legge previsti per la pubblicazione.
Le pagine web in cui sono esposti dati che presentano scadenze di pubblicazione devono impedire l'archiviazione e/o la cache da parte dei motori di ricerca (devono essere presenti i metadati del tipo <meta name="robots" content="noarchive">, oppure <meta name="robots" content="nocache"> o altri similari che possano essere sviluppati).
Eventuali file temporanei presenti nei personal computer vanno cancellati finito lo scopo per cui sono stati generati; eventuali file che servano per la tracciabilità di un processo, in quanto possono essere oggetto di audit, vanno conservati in modo ordinato in apposita cartella in "Gruppi".
I documenti cartacei, laddove necessario, vanno distrutti prima di essere messi nei cestini; nel caso in cui sia disponibile un distruggi documenti, si richiede di utilizzare questo strumento.
Definire una procedura per lo sfoltimento degli archivi locali delle sedi dell'Agenzia ed il conferimento di tale documentazione all'Archivio Deposito. In linea di massima potranno essere conferite, dopo apposita catalogazione, le pratiche "chiuse", non più oggetto di trattamento se non sporadico ed improbabile (es. per motivi di ricorso legale).
Le domande ed istanze di aiuto vengono smaltite secondo le indizioni della sopraintendenza ai beni culturali ed archivistici.

29151-A.11.4 – Monitoraggio ed audit

La matrice di analisi dei rischi GDPR viene rianalizzata con cadenza biennale, o annualmente in caso di modifiche rilevanti, in concomitanza con l'analisi dei rischi per la ISO27001.

29151-A.8 – Accuratezza e qualità del dato

Nelle attività di collaudo degli applicativi deve essere valutato l'impatto delle nuove implementazioni sull'integrità dei dati esistenti e le garanzie di integrità dei nuovi dati che saranno gestiti.

Nelle attività di collaudo dei sistemi di interscambio automatico deve essere valutato l'impatto delle nuove implementazioni sull'integrità dei dati esistenti e le garanzie di integrità dei nuovi dati che saranno gestiti.
Nel progetto di sistemi di integrazione si preferirà utilizzare la scrittura su tabelle "di confine" e non direttamente sulla produzione, per avere il controllo su cosa viene scritto e da chi. Deve essere previsto un controllo a campione sul set di dati acquisiti, da parte di soggetti diversi dagli esecutori dell'aggiornamento attraverso la consultazione delle diverse banche dati di riferimento.