AGEA

REQUISITI GENERALI IN MATERIA DI SICUREZZA DELLE INFORMAZIONI CUI GLI "ENTI DELEGATI" DEVONO FAR RIFERIMENTO DURANTE LO SVOLGIMENTO DELLE ATTIVITÀ OGGETTO DI CONVENZIONE CON AGEA

			Data
Versione		1.2	*21/09/2020*

	Struttura	Responsabile	*Data*	*Firma*
Redatto	Responsabile Sistema di gestione ISO27001	L. De Lorenzo		Firmato digitalmente da: Lamberto De Lorenzo Data: 23/09/2020 12:05:18
Verificato	Responsabile Sicurezza delle informazioni ISO 27001	C. Di Iorio		DI IORIO COSTANTINO AGEA - AGENZIA PER LE EROGAZIONI IN AGRICOLTURA DIRIGENTE 23.09.2020 15:52:36 UTC
Approvato	Rappresentante della Direzione per il sistema di gestione della sicurezza delle informazioni ISO 27001	F. Martinelli		MARTINELLI FRANCESCO AGEA - AGENZIA EROGAZIONE IN AGRICOLTURA DIRIGENTE GENERALE 25.09.2020 17:29:20 UTC

INDICE DEL DOCUMENTO

REGISTRO DELLE MODIFICHE

N° Revisione	Data	Descrizione	Autore
1.0	30/04/2020	Prima emissione	L. De Lorenzo
1.1.	08/07/2020	- Sono state meglio identificate la responsabilità della nomina del responsabile utenze (designato dal CAA e comunicato con atto formale ad AGEA). - sono stati riportati i sistemi di autenticazione digitale previsti dal CAD per la PA (es. SPID, CNS ecc..), attualmente utilizzati.	L. De Lorenzo
1.2	21/09/2020	Modificati alcuni aspetti formali presenti nel documento	L. De Lorenzo

REQUISITI GENERALI

1. INFORMAZIONI TRATTATE

Le informazioni trattate dall'Ente delegato in nome e per conto dell'Agenzia, quali ad esempio quelle relative alle domande di aiuto/pagamento, le informazioni per costituire ed aggiornare il fascicolo aziendale ovvero i documenti presentati dal produttore nell'ambito dei compiti assegnati all'Ente attraverso specifico contratto/convenzione con AGEA, devono essere trattate nel rispetto della normative vigente in tema di sicurezza e privacy e nel rispetto delle prescrizioni emanate da AGEA ed esclusivamente ai fini dello svolgimento delle attività delegate con il citato contratto/convenzione con AGEA.

L'Ente delegato ha l'obbligo di rispettare i requisiti di sicurezza e privacy stabiliti dalla Agea.

L'Ente delegato ha l'obbligo di fornire evidenza della puntuale trasmissione dei requisiti di sicurezza a tutto il personale utilizzato, alle sedi periferiche e ad eventuali subfornitori utilizzati affinché tutto il personale – anche appartenente ad altri enti/società - che tratta le informazioni per conto di Agea sia correttamente informato e formalmente impegnato al rispetto di tali requisiti.

Tutto il personale che tratta le informazioni deve essere adeguatamente informato e formato sui requisiti seguenti di sicurezza ed è tenuto a rispettare le prescrizioni di cui al Regolamento UE 2016/679 (*GDPR*) ed al Dlgs 196/03 e ss.mm.ii. Tutto il personale deve essere formalmente autorizzato ad effettuare i trattamenti dei dati personali assegnati.

Classificazione

Le informazioni che l'Ente delegato tratta per conto di Agea, devono essere classificate in relazione al loro valore, ai requisiti cogenti e alla criticità, ovvero all'entità del danno causato in caso di loro perdita, divulgazione o modifica non autorizzate.

Alle informazioni trattate dall'Ente Delegato per conto di Agea è stato assegnato un livello di classificazione "MEDIO" in quanto trattasi di:

- Informazioni che, se divulgate, possono comportare responsabilità di tipo amministrativo o danneggiare terze parti (*riservatezza*);
- Informazioni che, se alterate o diffuse con valori diversi da quelle reali, possono comportare disguidi o errori nello svolgimento di pratiche amministrative/istituzionali (*integrità*);
- Informazioni che, in caso di indisponibilità prolungata, possono comportare ripercussioni significative nello svolgimento dei procedimenti amministrativi/istituzionali di Agea (*disponibilità*);
- dati personali relativi al GDPR (Regolamento (UE) 2016/679) di tipo identificativo (riservatezza e integrità).

Alle informazioni relative ai dati giudiziari e di dati personali particolari ai sensi del GDPR trattate dall'ente delegato per conto di AGEA è attributo un livello di classificazione "ALTO" in quanto trattasi di:

- dati che, se divulgati, possono comportare per AGEA responsabilità di tipo penale o civile (riservatezza);
- dati che, se alterati o diffusi con valori diversi da quelli reali, comportano gravi errori nello svolgimento dei procedimenti istituzionali (integrità);
- dati che, in caso di indisponibilità anche per brevi periodi, comportano ripercussioni significative nello svolgimento dei procedimenti istituzionali di AGEA (disponibilità);
- dati personali di tipo sensibile e giudiziario (riservatezza e integrità).

I documenti cartacei che contengono le suddette informazioni a livello di classificazione MEDIO e ALTO, inclusi quelli giudiziari, sono classificati come "*Confidenziali*".

Inventario

Tutti gli asset associati alle informazioni e alle strutture di elaborazione delle informazioni che l'Ente delegato tratta per conto di Agea devono essere identificati; un inventario di questi asset deve essere compilato e mantenuto aggiornato.
In particolare, l'ente delegato deve pertanto mantenere aggiornato l'inventario dei seguenti asset presenti, sia presso le sedi centrali che periferiche:

- archivi cartacei;
- postazioni di lavoro e relative licenze software;
- eventuali dispositivi hardware laddove utilizzati (es: server, firewall, ecc) e relative licenze software

Controllo accesso fisico

Le aree dove vengono gestite le informazioni che l'Ente delegato tratta per conto di Agea (uffici, archivi, CED… laddove utilizzati) devono essere protette da appropriati controlli per l'ingresso atti ad assicurare che solo il personale autorizzato abbia il permesso di accedervi.

2. MISURE DI SICUREZZA PER PROTEGGERE LE INFORMAZIONI SU SUPPORTO INFORMATICO

Le informazioni trattate con strumenti informatici che abbiano un livello di classificazione MEDIO, devono essere protette con le seguenti misure di sicurezza minime:

- Le informazioni devono essere protette da accessi non autorizzati.
- In generale bisogna tracciare gli accessi alle informazioni e le operazioni di modifica delle stesse.
- verificare che siano applicate le misure previste dal "Disciplinare tecnico in materia di misure minime di sicurezza" allegato B del D.L. 196/03 e ss.mm.ii, anche se abrogato nella versione novellata dal D.lgs n. 101 del 10 agosto 2018.
- Verificare che siano applicate le misure di sicurezza a protezione dei dati personali di tipo identificativo indicate nel documento REGISTRO DELLE ATTIVITA' DI TRATTAMENTO DI DATI PERSONALI (Articolo 30 del Regolamento Europeo n. 679/2016 - GDPR)/lettere di nomina a responsabile e/o da implementare a fronte dell'analisi dei rischi da condurre per valutare i rischi per i diritti e le libertà degli interessati.
- Verificare se siano applicabili per i sistemi che trattano le informazioni per conto di Agea e, in caso positivo, verificare che siano applicate le misure di sicurezza obbligatorie riportate nella Circolare 18 aprile 2017, n. 2/2017 emessa dall'AgID in attuazione della Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015 (MISURE MINIME DI SICUREZZA ICT PER LE PUBBLICHE AMMINISTRAZIONI) e rientranti nel Livello "Minimo"
- verificare che siano applicate le misure previste dal Garante della privacy con il provvedimento "Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali - 13 ottobre 2008" sulla corretta dismissione degli apparati elettronici contenenti dati personali.
- Effettuare copie di backup dei dati con periodicità adeguata.

3. MISURE DI SICUREZZA PER PROTEGGERE LE INFORMAZIONI SU SUPPORTO CARTACEO

Il personale deve osservare - nella gestione della documentazione cartacea - le seguenti norme comportamentali:

- I documenti cartacei, non classificati come pubblici, presenti presso i locali degli uffici devono essere conservati in maniera che ad essi non accedano persone prive di autorizzazione.
- Qualora il personale abbandoni temporaneamente la postazione di lavoro deve preoccuparsi di non lasciare incustodito e visibile, a chi non è autorizzato, alcun

documento cartaceo che non sia classificato pubblico, e deve attivare le opportune precauzioni a tutela della riservatezza dei documenti

- Al termine della giornata lavorativa la documentazione non classificata come pubblica deve essere riposta nei luoghi di conservazione previsti in base alla classificazione di sicurezza assegnata (armadi e cassetti con o senza serratura, cassaforte, ecc.), come successivamente indicato.
- La documentazione cartacea non deve essere riprodotta o divulgata per fini diversi da quelli per cui è stata prodotta come previsto nel contratto/convenzione con AGEA.
- Il personale in possesso di documentazione cartacea non classificata come pubblica deve rispettare la riservatezza ed il segreto d'ufficio
- La documentazione cartacea non classificata come pubblica spedita via posta, interna o esterna, deve essere chiusa in un involucro. L'involucro deve riportare l'indirizzo del mittente e del destinatario e non deve permettere l'accesso visivo alle informazioni in esso contenute.
- I documenti cartacei classificati come **"diffusione limitata"** devono essere conservati in armadi o in cassetti e non tenuti sulle scrivanie delle singole persone, nel rispetto della politica della scrivania pulita.
- I documenti cartacei classificati come **"confidenziali"** devono rispettare le seguenti misure di sicurezza minime:
  - devono essere conservati in appositi armadi o cassettiere protetti;
  - possono essere trasmessi o riprodotti solo previa autorizzazione;
  - possono essere trasmessi verso soggetti esterni solo previa definizione di accordi di sicurezza e con modalità sicure di trasferimento;
  - la loro distruzione deve avvenire per sminuzzamento tramite appositi strumenti.

4. MISURE DI SICUREZZA PER L'ACCESSO AL SIAN

Gestione formale delle utenze per l'accesso al SIAN

L'Ente Delegato deve individuare un "*Responsabile delle utenze*", designato e comunicato con atto formale ad AGEA, quale soggetto responsabile dell'assegnazione delle utenze per l'accesso al sistema SIAN agli utenti incaricati dello svolgimento delle attività delegate all'Ente delegato.
L'attribuzione delle utenze su sistema SIAN deve essere effettuata nel rispetto del principio della separazione delle funzioni e in ottemperanza alle norme previste in merito a tale principio dai Regolamenti vigenti.
Il processo deve includere almeno i seguenti requisiti di sicurezza:

- Gli utenti devono essere tenuti a firmare una dichiarazione (per credenziali SIAN) che li impegni a mantenere riservate le informazioni segrete di autenticazione o ad utilizzare sistemi di autenticazione digitale previsti dal CAD per la PA (es. SPID, CNS ecc..);
- Le informazioni segrete di autenticazione, laddove consegnate agli utenti devono avere validità temporanea e devono essere cambiate al primo utilizzo;

- Deve essere verificata l'identità di un utente prima di fornire, rimpiazzare o sostituire nuove informazioni segrete di autenticazione;
- Le informazioni segrete di autenticazione temporanee, devono essere consegnate agli utenti in modo sicuro;
- Gli utenti devono confermare la ricezione delle informazioni segrete di autenticazione;
- Le informazioni segrete di autenticazione di default dei produttori devono, se possibile, essere modificate a seguito dell'installazione di sistemi o software.

Per il dettaglio operativo si può fare riferimento alla procedura definita nel documento di AGEA "*ZGA-X-K6-001 Procedura Gestione Utenze SIAN*".

L'Ente delegato, mediante il suo Responsabile delle Utenze, ha l'obbligo di fornire trimestralmente il riesame delle utenze per l'accesso al sistema SIAN agli utenti incaricati dello svolgimento delle attività delegate all'Ente delegato.

Il responsabile delle utenze, nell'ambito dell'attività di riesame delle abilitazioni ai servizi del portale SIAN, deve formalizzare le responsabilità attribuite (titolarità degli utenti, aggiornamento delle abilitazioni, destinazione ad altri incarichi e revoche).

Norme comportamentali per il personale a cui sono assegnate le utenze per l'accesso al SIAN.

- Mantenere riservate le informazioni segrete di autenticazione, assicurandosi che non vengano divulgate a nessun'altra terza parte, incluso personale con autorità;
- Evitare di tenere una registrazione (ad esempio su carta, documenti software o dispositivi portatili) delle informazioni segrete di autenticazione, a meno che questa possa essere memorizzata in modo sicuro.
- Modificare le informazioni segrete di autenticazione ogni qualvolta vi sia un'indicazione della loro possibile compromissione;
- le password devono presentare le seguenti caratteristiche:
  - lunghezza minima sufficiente (almeno 8 caratteri);
  - non basate su qualcosa che qualcun altro possa facilmente indovinare od ottenere utilizzando informazioni relative alla persona, per esempio nomi, numeri di telefono e date di nascita, ecc.;
  - non vulnerabili ad attacchi a dizionario (es. non composte da parole incluse nei dizionari);
  - prive di caratteri consecutivi identici;
  - non formate da soli caratteri alfanumerici o numerici ma usando una combinazione di entrambi;
  - formate anche da caratteri speciali (es. [ ] @ #);
  - se temporanee, cambiate al primo log-on;
  - quando viene cambiata non sia uguale ad altre password precedentemente utilizzate.
- Non condividere informazioni segrete di autenticazione di utenti individuali;

- Assicurare un'adeguata protezione delle password quando sono memorizzate in procedure automatiche di log-on;
- Non usare le stesse informazioni segrete di autenticazione per scopi aziendali e non.

5. GESTIONE DEGLI INCIDENTI

Nel caso si verificassero incidenti di sicurezza relativamente ai dati oggetto di trattamento da parte dell'Ente delegato (furto di identità, accesso non autorizzato al SIAN, furto di documenti, perdita di documenti, accesso non autorizzato a documenti, utenza non disabilitata se l'utente a cui è stata assegnata non è più autorizzato ad accedere al SIAN, etc.), l'Ente delegato deve immediatamente segnalare l'incidente al Responsabile sicurezza delle informazioni di Agea tramite la casella di posta **servizio.sicurezza@sin.it**, il quale provvederà anche a valutare, d'intesa con il Responsabile della protezione dei dati (RPD) di AGEA, se si tratti anche di una violazione dei dati personali per attivare eventuali azioni conseguenti ai sensi di quanto previsto agli art. 33 e 34 del GDPR in accordo ai documenti S-AGE-SSGE-L5-16002 Procedura per la Gestione degli Incidenti di sicurezza e S-AGE-SSGE-L5-18001 Procedura per il Personal Data Breach Management.
Nel caso in cui l'Ente delegato, nominato da AGEA Responsabile del trattamento dei dati personali, ritenga, da una prima analisi, che si tratti di Data Breach è tenuto anche ad informare tempestivamente e senza ingiustificato ritardo, entro 24 ore dall'avvenuta conoscenza dell'evento, il Titolare del trattamento dei dati AGEA ed il RPD AGEA. Tale notifica – da effettuarsi ad AGEA sia tramite PEC all'indirizzo protocollo@pec.agea.gov.it che tramite mail all'indirizzo ageaprivacy@agea.gov.it – deve essere accompagnata da ogni documentazione utile per permettere ogni valutazione e azione di competenza.

6. AUDIT

L'Ente delegato, al fine di verificare la corretta applicazione delle misure di sicurezza, è oggetto di controlli di audit da parte della UE e/o di AGEA tramite personale proprio o soggetto terzo appositamente nominato.

L'Ente delegato deve effettuare opportuni controlli, anche tramite audit, affinché eventuali soggetti sub-delegati/sub fornitori rispettino le misure di sicurezza indicate e su richiesta deve fornire evidenza di tali controlli.

In particolare per il campionamento e la priorità di verifica delle proprie sedi periferiche, deve adottare una procedura oggettiva che si basi su i criteri di rischio e di rilevanza. Per definire tali criteri si suggerisce di basarsi sui seguenti elementi:

- n° di sedi territoriali;
- n° atti amministrativi trattati;
- dimensione economica degli aiuti gestiti;
- categoria dei dati personali trattati (dati particolari ecc.):
- eventuali non conformità rilevate in precedenza nel corso di audit svolti dall'ente delegato stesso, da AGEA o da soggetti terzi incaricati, che siano noti;

- risultati del *Risk Assessment* in materia di Privacy (PIA) e/o Sicurezza delle Informazioni effettuato in proprio dall'ente delegato (ove applicabile) o reso disponibile da AGEA;
- risultati degli Audit eseguiti dall'Organismo di Certificazione relativamente alla norma ISO 27001 (ove applicabile);
- valutare eventuali non conformità non risolte su audit pregressi o ritardi nella definizione ed implementazione delle azioni correttive e di miglioramento.

7. CONTINUITA' OPERATIVA

L'Ente delegato deve stabilire, documentare, ed attuare procedure per assicurare la continuità dei servizi oggetto di delega durante il verificarsi di una situazione avversa.