ORGANISMO PAGATORE
UFFICIO MONOCRATICO

Via Palestro, 81 – 00185 Roma
Tel. 06/494991 Fax 06/4453940

Agea
Agenzia
per le Erogazioni
in Agricoltura

Ai CAA

Alle Regioni

e, p.c. al Responsabile della sicurezza
delle informazioni
c.a. dott. G. Vulpes

Oggetto: Requisiti di sicurezza ISO 27001.

Premesso che:

- il Regolamento Delegato n. 907/2014 della Commissione Europea dell'11 marzo 2014, che integra il regolamento (UE) n. 1306/2013 del Parlamento europeo e del Consiglio, stabilisce che "*A decorrere dal 16 ottobre 2016 la sicurezza dei sistemi d'informazione è certificata in conformità con l'Organizzazione internazionale per la standardizzazione 27001: Sistemi di gestione della sicurezza delle informazioni - Requisiti (ISO)*";

- il DM 12/01/2015 n. 162 relativo alla semplificazione della gestione della PAC 2014 - 2020, all'art. 2, c.2, stabilisce che "*A tale fine, gli Organismi Pagatori hanno l'obbligo, dal 2016, di attuare la certificazione delle informazioni secondo la norma ISO/IEC 27001*";

- il documento della Commissione MEMORANDUM TRASMESSO AL COMITATO DEI FONDI AGRICOLI - Certificazione degli organismi pagatori secondo la norma ISO 27001- D(2015)AGRI/2015/agri.ddg4.j.1(2015)1359224-IT-MEMO stabilisce che "*Le norme dell'Unione prevedono la possibilità di delegare taluni compiti (ovvero le attività operative) dell'organismo pagatore (allegato I, punto 1., parte C), del regolamento (UE) n. 907/2014). Gli organismi delegati possono scegliere di non essere certificati secondo la norma ISO 27001. Tuttavia tali organismi provvedono al trattamento e alla gestione di dati che appartengono all'organismo pagatore. L'integrità, la riservatezza e la disponibilità di tali dati devono essere sufficientemente garantite. In questo specifico caso diventano applicabili disposizioni sostitutive in materia di sicurezza dei sistemi d'informazione. Poiché l'organismo pagatore rimane responsabile della sicurezza dei sistemi d'informazione*

qualunque sia il livello di delega, esso deve garantire che il livello di sicurezza delle informazioni presso l'organismo delegato sia identico a quello richiesto all'organismo pagatore stesso. Pertanto l'organismo pagatore deve provvedere affinché tutti gli accordi conclusi con gli organismi delegati prevedano requisiti di sicurezza delle informazioni (ad esempio inserendo nell'accordo sul livello di servizio i requisiti in materia di monitoraggio e comunicazione, il diritto di audit, ecc.)";

al fine di garantire la riservatezza, integrità e disponibilità delle informazioni gestite con riferimento all'erogazione di aiuti, contributi, premi ed interventi alle imprese dell'Organismo Pagatore AGEA, è necessario che ciascun ente delegato svolga le attività affidate da AGEA in accordo alle Politiche di Sicurezza ed ai requisiti di sicurezza indicati dalla scrivente, in accordo allo standard ISO 27001 ed alla normativa vigente in tema di privacy.

Pertanto, si trasmettono in allegato i requisiti di sicurezza definiti che costituiscono parte integrante e sostanziale degli accordi stipulati tra AGEA e codesti Enti. Eventuali loro modifiche/integrazioni potranno essere comunicate successivamente con specifica lettera.

Si resta in attesa di copia controfirmata della presente che valga quale formale accettazione di quanto comunicato.

Il Direttore dell'Ufficio Monocratico dell'O.P.
Maurizio Salvi

ALLEGATO 1 - Requisiti in materia di sicurezza delle informazioni cui gli "Enti delegati" devono far riferimento durante lo svolgimento delle attività oggetto di convenzione con Agea.

1. Dati trattati

I dati trattati dall'Ente delegato in nome e per conto dell'Agenzia, quali ad esempio quelli relativi alle domande di aiuto/pagamento, i dati per costituire ed aggiornare il fascicolo aziendale ovvero i documenti presentati dal produttore nell'ambito dei compiti assegnati all'Ente, devono essere trattati nel rispetto della normative vigente in tema di sicurezza e privacy e nel rispetto delle prescrizioni emanate da AGEA.

Ai suddetti dati è stato assegnato un livello di classificazione MEDIO (ad eccezione di eventuali dati giudiziari a cui è attributo un livello di classificazione alto) ovvero:

- dati che, se divulgati, possono comportare responsabilità di tipo amministrativo o danneggiare terze parti (riservatezza);
- dati che, se alterati o diffusi con valori diversi da quelli reali, possono comportare disguidi o errori nello svolgimento di pratiche amministrative/istituzionali (integrità);
- dati che, in caso di indisponibilità prolungata, possono comportare ripercussioni significative nello svolgimento dei procedimenti amministrativi/istituzionali di Agea (disponibilità);
- dati personali relativi al Codice in materia di protezione dei dati personali (Dlgs. 196/03) di tipo identificativo e comune (riservatezza e integrità).

I documenti cartacei che contengono i suddetti dati, inclusi quelli giudiziari, sono classificati come "*Confidenziali*".

2. Misure di sicurezza per proteggere i dati su supporto informatico

I dati trattati con strumenti informatici, dato il suddetto livello di classificazione MEDIO, devono essere protetti con le seguenti misure di sicurezza minime:

- le informazioni devono essere protette da accessi non autorizzati;
- devono essere tracciati gli accessi alle informazioni e le operazioni di modifica delle stesse;
- devono essere applicate le misure previste dal "*Disciplinare tecnico in materia di misure minime di sicurezza*" allegato B del Dlgs.196/03.
- devono essere 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;
- devono essere effettuate copie di backup dei dati con periodicità adeguata.

3. Misure di sicurezza per proteggere i dati su supporto cartaceo

I documenti cartacei, dato il livello di classificazione CONFIDENZIALE loro assegnato, 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.

Il personale autorizzato ad accedere a tali documenti deve osservare nella gestione della documentazione cartacea le seguenti norme comportamentali:

- I documenti cartacei 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 deve essere riposta nei luoghi di conservazione previsti in base alla classificazione di sicurezza assegnata (armadi e cassetti con o senza serratura, cassaforte, ecc.).
- La documentazione cartacea non deve essere riprodotta o divulgata per fini diversi da quelli per cui è stata prodotta.
- Il personale in possesso di documentazione cartacea deve rispettare la riservatezza ed il segreto d'ufficio, secondo le norme previste dal Contratto Collettivo Nazionale dei Dipendenti Pubblici e dal D.lgs. 196/2003.
- La documentazione cartacea 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 prodotti 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 prodotti classificati come "confidenziali" devono essere conservati in armadi protetti, cioè tenuti chiusi a chiave, conservata dall'utilizzatore della documentazione o dal suo responsabile.
- I documenti classificati come "confidenziali" possono essere consegnati a soggetti esterni solo se è stato stabilito tra le parti un accordo formale di riservatezza che definisca anche i requisiti di sicurezza da garantire.
- I documenti classificati come "confidenziali" possono essere consegnati a soggetti esterni solo secondo modalità di sicurezza appositamente concordate.
- La diffusione non autorizzata, la perdita, la manomissione, la sottrazione o l'uso indebito di informazioni classificate al livello "confidenziale" costituisce un "incidente di sicurezza" e pertanto deve essere segnalato ad AGEA nella persona del Responsabile sicurezza delle informazioni.

4. Misure di sicurezza per l'accesso al SIAN

Gestione formale delle utenze per l'accesso al SIAN

E' necessario definire ed adottare un processo di gestione formale per l'assegnazione di informazioni segrete di autenticazione (codice utente, password, PIN, ecc.).

L'Ente Delegato deve individuare e nominare con atto formale il "*Responsabile delle utenze*" quale soggetto responsabile dell'assegnazione delle utenze per l'accesso al sistema SIAN ai funzionari 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 UE n. 1306/2013 e n. 1305/2012 e dai rispettivi regolamenti delegati e di esecuzione e s.m.i.

Il processo deve includere i almeno i seguenti requisiti di sicurezza:

- Gli utenti devono essere tenuti a firmare una dichiarazione che li impegni a mantenere riservate le informazioni segrete di autenticazione.
- Le informazioni segrete di autenticazione 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*".

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

1. Mantenere riservate le informazioni segrete di autenticazione, assicurandosi che non vengano divulgate a nessun'altra terza parte, incluso personale con autorità.
2. 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.
3. Modificare le informazioni segrete di autenticazione ogni qualvolta vi sia un'indicazione della loro possibile compromissione.
4. Le password devono presentare le seguenti caratteristiche:
   - lunghezza minima di 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.
5. Non condividere informazioni segrete di autenticazione di utenti individuali.
6. Assicurare un'adeguata protezione delle password quando sono memorizzate in procedure automatiche di log-on.
7. 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.

6. Audit

L'Ente delegato, al fine di verificare la corretta applicazione delle misure di sicurezza, può essere oggetto di visite di audit da parte della UE ovvero di AGEA tramite personale proprio o soggetto terzo appositamente nominato.