

CAMPAGNA/ESERCIZIO FINANZIARIO

DICHIARAZIONE

Il Sottoscritto/a _____, nato/a a _____ prov. _____
il _____, residente in Via _____ n° _____
Comune _____, Prov. _____,
Cod. fiscale _____,

[compilare una delle tre casistiche sotto indicate]

- ☐ professionista iscritto all'ALBO/Collegio _____ della provincia di _____ con n° _____ che intrattiene un rapporto contrattuale con _____ affidato in data _____ per effettuare le attività di: _____
- ☐ dipendente di _____ che intrattiene un rapporto contrattuale con _____ affidato in data _____ per effettuare le attività di _____
- ☐ ALTRO(specificare) _____ per effettuare le attività di _____

consapevole che potranno essere effettuati controlli sulla veridicità delle dichiarazioni rese; che, ai sensi dell'art. 75 del D.P.R. 28/12/2000, n. 445, in caso di dichiarazione mendace decadrà dal beneficio ottenuto sulla base della dichiarazione non veritiera; consapevole, altresì, delle sanzioni penali richiamate dall'art. 76 del predetto Decreto legislativo:

DICHIARA SOTTO LA PROPRIA RESPONSABILITA':

1) Titolarità domanda (*barrare una sola voce*):

- ☐ di **NON essere titolare** di alcuna domanda di sostegno/pagamento
☐ di **essere titolare** della/e domanda/e di sostegno/pagamento riportate in **Allegato 1**

2) Compartecipazioni finanziarie e/o patrimoniali

- ☐ di **NON** non avere compartecipazioni finanziarie e/o patrimoniali in ditte, imprese e aziende agricole collegate direttamente od indirettamente o con singoli beneficiari titolari di domande di sostegno/pagamento del cui controllo potrà essere incaricato
☐ di **AVERE** compartecipazioni finanziarie e/o patrimoniali in ditte, imprese e aziende agricole collegate direttamente od indirettamente o con singoli beneficiari titolari di domande di sostegno/pagamento, del cui controllo potrà essere incaricato, riportate in **Allegato 2**

3) Di **non avere motivi ostativi al corretto svolgimento dell'attività**, con particolare riferimento a rapporti od interessenze con C.A.A., con Associazioni professionali agricole, con organizzazioni di produttori, con Associazioni o Enti ad esse collegate direttamente od indirettamente o con singoli produttori titolari di domande di sostegno/pagamento ubicate nei territori per i quali svolge l'attività;

4) Di non svolgere attività professionale in conflitto di interessi con la funzione di controllo delle domande del cui controllo è incaricato

5) [solo nel caso di professionista agronomo iscritto ad albo/collegio] Di **firmare e timbrare** le relazioni di controllo con il proprio timbro dell'Ordine/collegio professionale di appartenenza;

6) Di avere **ricevuto copia delle Specifiche tecniche** secondo le quali dovranno essere effettuate le attività di cui sopra;

7) Di **essere disponibile ai Controlli di Qualità ed eventuali collaudi** anche successivamente alla chiusura delle attività;

8) Di comunicare tempestivamente qualunque variazione si verifichi nel corso del rapporto contrattuale a quanto comunicato nella presente dichiarazione;

9) di non essere mai stato implicato in procedimenti giudiziari relativi a reati di cui al D.Lgs. 231/2001 ed alla L. 190/2012.

10) Di ottemperare ai requisiti in materia di privacy e sicurezza delle informazioni in accordo allo standard ISO IEC 27001, con specifico riferimento a quanto di seguito riportato:

Documento a diffusione limitata-

1. Dati trattati

I dati trattati in nome e per conto di AGEA durante l'espletamento delle attività contrattualmente previste ovvero i documenti gestiti nell'ambito dei compiti assegnati, devono essere trattati nel rispetto delle prescrizioni emanate da AGEA con riferimento alle normative vigenti in tema di sicurezza e privacy (in particolare il Reg.UE 2016/679). 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 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 Garante della Privacy con il Provvedimento "Rifiuti di apparecchiature elettriche ed elettroniche (Raee) 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 almeno settimanale

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

I documenti cartacei 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 deve essere mantenuta riservata e non deve essere riprodotta o divulgata per fini diversi da quelli per cui è stata prodotta.
- 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 al Responsabile sicurezza delle informazioni (vedi par. 5)

4. Misure di sicurezza 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 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.
- Non condividere informazioni segrete di autenticazione di utenti individuali né permetterne l'utilizzo ad altri utenti;
- 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 (quali, a titolo esemplificativo: furto di identità, 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'incidente deve essere immediatamente segnalato al Responsabile sicurezza delle informazioni.

6. Audit

Al fine di verificare la corretta applicazione delle misure di sicurezza possono essere previste visite di audit da parte di AGEA tramite personale proprio o soggetto terzo appositamente nominato.

Fatto a _____

Data _____

In fede.**Firma** _____**ALLEGATO 1****Elenco** della/e domanda/e di sostegno/pagamento di cui è titolare**ALLEGATO 2**

Elenco compartecipazioni finanziarie e/o patrimoniali in ditte, imprese e aziende agricole collegate direttamente od indirettamente o con singoli beneficiari titolari di domande di sostegno/pagamento del cui controllo potrà incaricato

Fatto a _____

Data _____

In fede.**Firma** _____

Documento a diffusione limitata-

Il Sottoscritto autorizza la gestione dei dati personali ai sensi del Reg.UE 2016/679 per le finalità di governo, controllo, sicurezza, audit e verifica di conformità delle attività operative svolte in ambito SIAN. I dati saranno solo per il tempo necessario ad eseguire il trattamento per le finalità menzionate e per tutta la durata del contratto tra RTI lotto 2 e Agea, e sino a quando persistano obbligazioni o adempimenti connessi all'esecuzione dello stesso. Essi potranno essere comunicati al personale RTI lotto 2, di AGEA, di SIN, del MIPAAF e degli enti collegati, delle aziende costituenti il RTI lotto2 e all'autorità giudiziaria a fini di indagine.

firma _____

Documento a diffusione limitata-